ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework

Kai Lin Tay

June 2023

IISS
The International Institute
for Strategic Studies

Contents

Executive Summary

Cyber threats in Southeast Asia have been increasing in quantity and sophistication for at least the last decade. This is driven by a number of factors, ranging from the rise in connectivity accelerated by the COVID-19 pandemic, greater adoption of advanced technologies such as artificial intelligence and cloud computing, and the growing status of the region as a cyber-espionage target due to its rising geopolitical significance.

This report seeks to provide an overview of the current state of cyber-security cooperation between countries of the Association of Southeast Asian Nations (ASEAN) and to address the issue of regional response to cyber emergencies in the Southeast Asian context. By examining cyber-emergency-response models in the European Union and the United States, the report identifies gaps in ASEAN's current cyber-security-cooperation architecture and proposes key areas of development required in order to establish a cyber-emergency framework for the region. The report's findings also support ASEAN's long-term goal of implementing United Nations (UN)-recommended norms in the area of mutual assistance during a cyber attack.

There are high levels of cooperation among ASEAN member states on computer emergency response teams (CERTs) thanks to efforts made in the early 2000s to boost the region's ICT sector. However, only in recent years has ASEAN moved towards formalising existing CERT cooperation. While cyber-security issues used to be treated under broader economic and political-security platforms, there are now dedicated platforms established to discuss cyber-security intra- and extra-regionally.

The report also focuses on the issue of critical information infrastructure (CII) protection during a cyber emergency. In the last five years, several initiatives involving dialogue partners, international organisations and the private sector have been established to enhance regional cyber-security capacities and strengthen mutual trust among ASEAN member states. Within the region, Singapore and Malaysia have played critical roles spearheading multi-stakeholder capacity-building initiatives and establishing information-sharing mechanisms in the financial and defence sectors.

While information-sharing and capacity-building measures have boosted the region's preparedness for cyber attacks against CII, as long as ASEAN's overall cyber-security architecture remains fragmented this will frustrate further progress. Not only are member states at varying levels of cyber-security maturity, but the region also lacks a common cyber lexicon and sufficient numbers of cyber-security professionals, and has not agreed on a strategic approach towards cyber security.

The report identifies key steps towards creating an ASEAN cyber-emergency-response framework. It recommends identifying priority CII sectors in each member state, as well as strengthening regional support for UN-recommended cyber norms.

In an increasingly connected world, building a cyber-emergency-response framework for ASEAN is a timely measure to boost cyber resilience across the region, while also ensuring that assistance is accorded to member states with less capacity for dealing with cyber crises.

Introduction

This report seeks to address the issue of regional response to cyber emergencies in the Southeast Asian context. Specifically, it aims to shed light on the gaps hindering effective regional response by members of the Association of Southeast Asian Nations (ASEAN) to a cyber emergency – an attack targeting national or cross-border critical information infrastructure (CII). Most of the literature covering cyber-security issues focuses on the European context, and studies covering the Southeast Asian region are relatively few. Scholarly work that does tackle cyber security in ASEAN states largely revolves around cyber policy, cyber diplomacy, cyber resilience or norms-building, while literature on cyber emergency is lacking. This paper aims to fill these knowledge gaps by examining the limitations in ASEAN cyber-security-cooperation architecture that hamper it from forming a cyber-emergency-response framework like those established in the United States (US) and the European Union (EU). Such a framework would contribute towards the operationalisation of the United Nations (UN) Group of Governmental Experts on Developments in the Field of Information and Communications in the Context of International Security norms, in particular the suggested norm on emergency assistance to other states, which recommends that:

> 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.[1]

Defining Cyber Emergency and Critical Information Infrastructure

One of the key issues facing any sort of national or international response to cyber incidents is determining the threshold at which a cyber incident is designated an 'emergency' or 'crisis'.[2] As ASEAN has not developed its own cyber-security operational language, this report's definition of 'cyber emergency' is informed by US and EU classifications.

The United States' Department of Homeland Security classifies cyber incidents into five levels of severity.[3] A cyber incident at the 'emergency' level poses 'an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens'.[4] In contrast, the EU Agency for Cybersecurity (ENISA) does not classify cyber incidents into discrete tiers. It defines a cyber-security incident as a 'crisis' when 'the disruption caused by the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level'.[5]

This report will similarly discuss multinational response to cyber incidents threatening critical information infrastructure. It defines a cyber emergency or cyber crisis as cyber incidents that poses an imminent threat, or causes actual disruption to, a wide range of critical information infrastructure in one or more member states, resulting in severe national or cross-border economic, social or national-security impacts. 'Critical information infrastructure' here refers to the interconnected systems and networks serving a country's critical infrastructure sectors – such as energy, transportation, digital infrastructure, financial services, health, water and agriculture – the disruption of which will have debilitating social, political or economic effects.[6]

The Cyber Threat Landscape in Southeast Asia

Cyber attacks in Southeast Asia are increasing in prevalence and sophistication as digitalisation permeates all parts of society, from government and the military to the financial and healthcare sectors. Even before the COVID-19 pandemic, critical information infrastructure had been the target of cyber attacks. In 2017, at least two of Indonesia's major hospitals were hit by

the WannaCry ransomware in an attack that affected over 100 countries globally.[7] As a regional hotspot for maritime conflict and great-power rivalry, CII sectors in Southeast Asia – including energy, telecommunications, finance, transportation, defence and government entities – have for over a decade been prime targets for state-linked advanced persistent threat (APT) actors to siphon state secrets and sensitive corporate data.[8] For example, a recent report by Symantec revealed a cyber-espionage campaign by China-linked hackers targeting the supervisory control and data acquisition (SCADA) systems[9] of a water company, a power company, a communications company and a defence organisation in the region.[10] Moreover, these APTs constantly adapt their tactics, techniques and procedures to establish a permanent presence in high-value networks.[11]

One cause of intensifying attacks on CII is the accelerated pace at which industrial control systems (ICS) within CII across Southeast Asia are being connected to the internet in a bid to improve the efficiency and reliability of operational processes. Legacy ICS, which are generally more secure due to their isolated operational technology (OT) environment, have increasingly adopted modern IT software and systems that subject them to broader and more pervasive cyber threats emanating from external networks.[12] The converging IT/OT landscape is growing more complex with the emergence of Industry 4.0 ecosystems, which leverage advanced digital technologies such as artificial intelligence, robots, cloud computing, and the Industrial Internet of Things (IIoT), introducing significantly more vulnerabilities.[13] Additionally, in light of ASEAN's ongoing plans to enhance connectivity[14] on a regional level, cross-border dependencies and interdependencies[15] among member states' CII are bound to deepen, exacerbating threat perceptions of individual members.

The onset of the COVID-19 pandemic accentuated existing cyber threats[16] through an unprecedented proliferation of attack surfaces arising from the need for remote services and operations such as online health consultation and online payments. Small- and medium-sized enterprises prioritised digital transformation in order to circumvent the barriers imposed on physical mobility, with some paying little or no heed to security considerations when moving their operations online.[17] For CII owners, there is also a growing imperative to remotely maintain their assets and services through use of IIoT sensors and the enterprise cloud.[18] A further cause of concern is that cyber attacks against CII are becoming an increasingly prevalent form of cyber crime.[19] In particular, incidents of ransomware attacking hospitals, medical institutions and insurance firms in Southeast Asia rose rapidly during the pandemic.[20]

Chapter One: ASEAN Cooperation in Cyber-security

CERT Cooperation

ASEAN governments have been bolstering computer emergency response team (CERT) cooperation among member states for more than a decade. The initial need for CERT cooperation arose from the broader economic imperative to strengthen and enhance the competitiveness of ASEAN's ICT sector. In 2000, ASEAN leaders signed the e-ASEAN Framework Agreement to establish a region-wide ASEAN Information Infrastructure[21] aiming at promoting the growth of regional electronic commerce, ICT trade and investments. Three years later, ASEAN ICT ministers agreed to develop and operationalise national CERTs by 2005 and develop a common framework for sharing expertise and cyber-security threat- and vulnerability-assessment information in real time.[22] As a result, most member states successfully established CERT operations by 2005 – though Cambodia and Laos only did so in 2008 and 2012 respectively.[23]

Building upon this foundation, subsequent initiatives focused on boosting regional technical response capabilities. In 2006, the first annual ASEAN CERT Incident Drill (ACID) was launched to strengthen cyber-security preparedness and cooperation among national CERTs. ASEAN ICT ministers also pledged in the 2006 Brunei Action Plan to intensify capacity-building and training programmes for all national CERTs and to strengthen the regional cyber-security network by including its dialogue partners in the ACID from 2007.[24] In 2011, the first five-year ASEAN ICT Masterplan (AIM 2015) established the ASEAN Network Security Action Council (ANSAC) to promote CERT cooperation. Through annual meetings with multiple stakeholders, key outcomes achieved in relation to CERT cooperation include the establishment of a common framework for network security and the development of an ASEAN cyber-security-incident handling and escalation procedure.[25]

Strengthening CERT cooperation was also a key goal repeated in AIM 2020, and during the period from 2015 to 2020, several projects were initiated under the aegis of the masterplan: the ASEAN CERT Maturity Framework;[26] a feasibility study on establishing an ASEAN Regional CERT; and the Incident Reporting Framework, which included templates and standardised responses to pre-identified threat levels.[27] The AIM 2020 action points survey revealed that ASEAN respondents perceived these CERT-related projects to be more valuable than developing regional frameworks for data protection and information security.[28]

However, it is unclear how many of these frameworks were adopted and implemented in individual member states. Moreover, strengthening CERT cooperation is a long-term and gradual process, as frameworks need to be periodically updated to encompass new technologies.

The ASEAN Digital Masterplan 2025 also seeks to expand existing CERT cooperation among member states by establishing a formal ASEAN Regional CERT by 2025.[29] In January 2021, ASEAN digital ministers began to move towards this goal by approving the establishment of the ASEAN CERT Information Exchange Mechanism, which will form a core component of the regional CERT.[30] While national CERTs in ASEAN member states already cooperate through platforms such as the ACID and the Asia-Pacific CERT, the establishment of the ASEAN CERT Information Exchange Mechanism will mark a shift towards the formalisation of existing national CERT-level exchanges and will help the region develop a coordinated technical response to significant cyber incidents. The ASEAN Regional CERT, which is due to be established in 2023/2024, will also strengthen the region's cooperation in critical information infrastructure protection (CIIP), including for cross-border CII such as maritime, communications and aviation.[31]

Regional Platforms for Cyber-security Cooperation

2016 marked a critical year in which cyber security was elevated as a standalone issue in its own right. That year, Singapore led the region to establish the Ministerial Conference on Cybersecurity (AMCC), the first, albeit informal, platform dedicated to discussing cyber-security

issues at the ministerial and senior-official level. Prior to this, cyber-security issues were discussed at various regional platforms for economic and political-security cooperation (see Table 1).[32] The ASEAN Defence Ministers' Meeting-Plus (ADMM-Plus) Cyber Security Expert Working Group (CS EWG) was also established in 2016, followed by the formation of the ASEAN Regional Forum (ARF) Inter-Sessional Meeting on the Security of and in the Use of ICT (ISM on ICTs Security) in 2017, which isolated cyber-security issues from the ARF Inter-Sessional Meeting on Counter-Terrorism and Transnational Crime.[33]

In October 2019, the fourth AMCC endorsed the creation of the ASEAN Cybersecurity Coordinating Committee (Cyber-CC),[34] which brings together representatives from cyber-security-related bodies as a formal body to coordinate cyber-security efforts and improve regional policy coherence.[35]

The creation of various cyber-security-focused platforms is a welcome development, paving the way for deeper coordination of ASEAN cyber-security efforts beyond the technical sphere to include diplomacy, policy and military aspects, which are integral for a multi-disciplinary issue like CIIP.

ASEAN Discourse on Cyber-security Cooperation: A New Focus on CIIP

In 2015, cyber security was given greater significance within ASEAN's overall ICT strategy when AIM 2020 listed 'information security and assurance' as an independent strategic thrust. Similar to the early 2000s, the primary motivation was economic – ASEAN aims to achieve a digitally enabled economy that is 'secure, sustainable and transformative.'[36] This strategic thrust aimed for the first time to 'develop regional cyber critical information infrastructure resilience practices', through which ASEAN can deploy a coordinated approach to CII protection and response.[37] This goal also reflects ASEAN's broad intent to deepen regional cyber-security collaboration beyond technical cooperation between national CERTs.

In April 2018, ASEAN leaders adopted the landmark 'Statement on Cybersecurity Cooperation', which tasked ASEAN ministers to coordinate 'cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts' across ASEAN's three pillars of cooperation (economic, political-security and socio-cultural).[38] The statement also called for the identification of a 'concrete list of voluntary, practical norms of State behaviour in cyberspace' and the facilitation of 'cross-border cooperation in addressing critical infrastructure vulnerabilities'.[39] To this end, ASEAN member states decided during the third AMCC in September 2018 to subscribe in-principle to the 11 voluntary, non-binding 2015 norms proposed by the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Communications in the Context of International Security, becoming the first and only regional grouping to date to do so.[40]

Table 1: **ASEAN cyber-security-related fora**

Platform	ASEAN pillar of cooperation	Areas of cooperation and related platforms
ASEAN Digital Ministers' Meeting (ADGMIN, formerly known as ASEAN TELMIN)	Economic	- Promotes ICT cooperation among ASEAN countries. - Published AIM 2011, AIM 2015 and AIM 2020, in which cyber security forms part of the wider portfolio of ICT issues, including improving ICT infrastructure, reducing the digital divide and improving cross-border trade within ASEAN. - ASEAN Telecommunications and IT Senior Officials Meeting (TELSOM) acts as the executive body to supervise, coordinate and implement policies relating to ICT cooperation under the directions and priorities set by TELMIN. - ASEAN Telecommunications Regulators' Council (ATRC) and ANSAC reside under the purview of TELMIN.
ASEAN Ministerial Meeting on Transnational Crime (AMMTC)	Political-security	- Prevents and combats transnational crime, including cyber crime. - Senior Officials' Meeting on Transnational Crime (SOMTC) acts as the executive body to coordinate and implement policies under the directions and priorities set by AMMTC. - SOMTC created a new working group on cyber crime in 2013.
ASEAN Regional Forum (ARF)	Political-security	- ASEAN-led extra-regional platform focusing on confidence building and preventive diplomacy in the Asia-Pacific region, including addressing criminal and terrorist use of cyberspace, and promoting stability and security in cyberspace. - Until 2017, cyber-security-related issues were discussed at the ARF Inter-Sessional Meeting on Counter-Terrorism and Transnational Crime.

Source: IISS

A working-level committee was also established to develop a long-term regional action plan for the practical implementation of the UNGGE norms, of which priority areas include CERT cooperation, protection of CII and mutual assistance in cyber security.[41]

During the fifth AMCC in 2020, the urgent need to protect national and cross-border CII in ASEAN was cast into the spotlight. In line with the 2018 leaders' statement, ASEAN member states agreed to take practical steps to improve regional cyber security, especially in protecting national and cross-border CII.[42] Thailand also shared the outcomes of its ASEAN Critical Information Infrastructure Protection Framework project, which was one of the key deliverables in AIM 2015.[43] The framework identified key steps for the development of ASEAN-wide initiatives to protect CII. One proposal was to establish a regulatory body to receive information from member states on individual CII sectors in order to create a region-wide information-sharing hub.

Regional Capacity-building and Confidence-building Measures

ASEAN has implemented several initiatives designed to enhance regional cyber-security capacities and strengthen mutual trust among member states. For instance, in terms of improving incident-response coordination, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) facilitates CERT-to-CERT information sharing and provides CERT-related training, including virtual cyber defence exercises.[44] The ASCCE also supports the socialisation of UN-recommended norms among member states via the UN-Singapore Cyber Fellowship Programme, launched in 2022. To maximise resources ASEAN capacity-building initiatives are designed to be open and inclusive, which they achieve by engaging dialogue partners, private-sector experts, international organisations and academia.

Japan is a long-time partner of ASEAN in boosting regional cooperation in CIIP. It hosted annual ASEAN-Japan CIIP workshops for member states from 2015–21 and organised annual cyber exercises with ASEAN from 2013–21,[45] which helped refine and strengthen coordination mechanisms during cyber incidents.[46] In 2016, the 9th ASEAN-Japan Information Security Policy Meeting acknowledged the third version of the Critical Information Infrastructure Protection guideline, a resource to help member states develop policies for their critical sectors.[47] Since 2018, member states have also benefitted from participating in the Japan-US Industrial Control Systems Cybersecurity Week training, along with other critical-infrastructure operators and cyber-security policymakers from the Indo-Pacific region.[48] Most recently, in 2020, Japan led ASEAN members, along with US and European countries, in an international digital defence exercise which required coordinated response to a simulation of a cyber attack on critical infrastructure systems.[49]

The ARF ISM on ICTs Security is a key platform in which ASEAN member states and dialogue partners have introduced several confidence-building measures (CBMs) that improve regional preparedness against cyber attacks. These include, among others, sharing of national strategies and laws, as well as sharing states' emergency-response plans for cyber incidents.[50] However, these measures are still in the early stages of development as member states and dialogue partners have only recently begun initial consultations. ASEAN states currently do not have a regional approach for identifying CII or developing cyber-related legislation for CII sectors. Some states, such as Cambodia and Laos, have yet to define their CII.

Nevertheless, ASEAN states have established cyber-information-sharing mechanisms in both the financial and defence sectors as part of regional CIIP. In 2019, the Central Bank of Malaysia led member states to establish the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP), which was fully operationalised in February 2021.[51] This platform allows ASEAN central banks to share cyber-threat intelligence and develop collaborative mitigating actions with ASEAN states which have engaged with the platform.

In the defence sector, the ADMM-Plus CS EWG has established a cyber Points of Contact and Technical Personnel Directory and a Glossary of Cyber Terminology, as well as a virtual platform for the group.[52] In June 2021, two major initiatives aimed at enhancing confidence building, information sharing and capacity building among ASEAN defence sectors were approved during the 15th ADMM.[53] The first is the ASEAN Cyber Defence Network (ACDN) proposed

by Malaysia. The ACDN aims to link all cyber defence operation centres of ASEAN defence establishments into a single network, providing a common communication platform among the points of contacts identified by the ADMM-Plus CS EWG. Importantly, the ACDN will also facilitate the exchange of knowledge and expertise between private-sector cyber experts and ASEAN cyber defence staff through physical visits, conferences and using virtual platforms.[54]

The second initiative – proposed by Singapore – is the establishment of the ADMM Cybersecurity and Information Centre of Excellence (ACICE). It mainly seeks to enable the ADMM to develop a deeper understanding of the cyber threat landscape through a shared platform that consolidates, synthesises and disseminates information about cyber security (including cyber malware, misinformation and disinformation).[55] Both initiatives are complementary and mutually supportive, and are guided by long-established ASEAN principles of respect for sovereignty and non-interference. It remains unknown as to how these two initiatives fit within existing collaborative bodies such as the ASCCE and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC). Nevertheless, while the specifics are still unclear, the decision to establish these two platforms underscores a common recognition by ASEAN defence establishments of the need to boost collective resilience and cooperation.

The ASEAN cyber-security cooperation initiatives discussed above, including the ASCCE and the ACDN, have engaged the private sector in capacity building or information sharing. Think tanks and academia, for example, the Council for Security Cooperation in the Asia Pacific, have also contributed to regional discussions on responsible behaviour in cyberspace through proposing CBMs which have been adopted by the ARF ISM on ICTs Security.[56] This reflects a common recognition of the limits of traditional state-based cooperation and thus a gradual shift towards including the private sector in regional cyber-cooperation efforts.[57] Public–private partnership in CIIP is most clearly observed in the financial-services sector. In 2016, the Monetary Authority of Singapore collaborated with the Financial Services Information Sharing and Analysis Center (a global financial industry consortium dedicated to reducing cyber risk) to establish the Asia Pacific Regional Intelligence and Analysis Centre.[58] This centre offers support to regional financial institutions, including several member states (Malaysia, Singapore and Thailand), in areas including threat intelligence, threat mitigation and technical-skills development.

ASEAN's collective measures for information sharing and capacity building have boosted the region's cyber-security preparedness against cyber attacks by improving policy coordination and collective incident response. However, ASEAN's overall cyber-security architecture remains fragmented – member states have varying levels of cyber readiness and there is an overall lack of strategic approach and institutional oversight, especially in CII sectors.[59] ASEAN notably lacks a collective approach to cyber-emergency response, including the ability to provide assistance or mitigate effects during a significant attack on a member state's CII or a cross-border CII. Chapter Three examines US and EU models for managing a coordinated response to cyber emergencies. Using these models, Chapter Four identifies ways in which a cyber-emergency-response framework could be built in the ASEAN context.

Chapter Two: Cyber-emergency-response Models

United States

The National Cyber Incident Response Plan published by the US Department of Homeland Security (DHS) in 2016 (NCIRP 2016) offers a broad strategic framework for how diverse stakeholders, including the government, private sector and international partners, can contribute resources to support a coordinated response to cyber incidents. Although the plan is targeted at 'significant cyber incidents' impacting critical infrastructure, the guidance that the NCIRP provides in coordinating structures and concurrent lines of effort is also applicable to responses to cyber emergencies, despite the latter requiring a greater degree of coordination.[60]

In the event of a significant cyber incident, private-sector entities or government agencies are encouraged to report the issue to established points of contact from a range of federal cyber-security agencies, law-enforcement authorities and Sector-Specific Agencies (SSA) – government agencies which possess sector-specific expertise and knowledge.

The lead federal cyber-security agencies – the Cyber Threat Intelligence Integration Center (CTIIC, under the Director of National Intelligence [DNI]), the National Cybersecurity and Communications Integration Center (NCCIC, under the DHS) and the National Cyber Investigative Joint Task Force (NCIJTF, under the Department of Justice [DOJ]) – make a joint assessment of the severity of the incident, in coordination with private-sector leadership and owners. If judged to be necessary, a Cyber Unified Coordination Group (UCG) is established to coordinate overall response. The Cyber UCG oversees three lines of effort – threat response, asset response and intelligence support. The DHS, through the NCCIC, is the lead agency in charge of asset response, which involves providing technical assistance to protect assets, mitigating vulnerabilities and assessing related risks to similar vulnerabilities. The DOJ, through the NCIJTF, deals with threat response, which includes law enforcement and national-security investigative activities. The DNI, through the CTIIC, is primarily in charge of intelligence support, which includes providing situational threat awareness, furnishing integrated analysis of trends in cyber threats and supporting interagency efforts to develop options to degrade or mitigate adversary threat capabilities.

Besides the lead agencies, the Cyber UCG also leverages SSAs in its response efforts. It establishes shared objectives for threat responses, asset responses and intelligence support to ensure unity of effort among federal agencies. Existing coordinating structures for routine cyber incidents are also integrated with the Cyber UCG to facilitate rapid sharing of information on incident response and recovery.[61]

The plan uses a sector-based approach in which 16 critical infrastructure sectors are identified,[62] each of which has routine coordinating structures in place for cyber incidents. A Sector Coordinating Council (SCC) is attached to each critical infrastructure sector. The council is a self-organised and self-governing private-sector entity that provides a platform for information sharing, analysis and collaboration regarding detection, prevention, mitigation and response to cyber incidents, not only across industry but also with government counterparts – the companion Government Coordinating Council (GCC) and the Sector-Specific Agency.[63]

Besides the SCC, private-sector critical infrastructure entities also coordinate regular cyber-security efforts through self-organised Information Sharing Analysis Centres (ISACs). The National Council of ISACs facilitates cross-sector coordination between the private sector and various government agencies. State, local, tribal and territorial (SLTT) government agencies can also be members of ISACs. As key critical-infrastructure operators, some of these government agencies help to direct and coordinate response work during a cyber incident. For cyber incidents specific to government networks, the Multi-State ISAC (MS-ISAC) acts as a focal point for information exchange and technical assistance within SLTT agencies as well as with the federal government.[64] In the event of a cyber incident that exceeds their

capabilities, SLTT government agencies can request additional resources from the federal government under frameworks such as the Stafford Disaster Relief and Emergency Assistance Act.[65]

During a significant cyber incident, enhanced coordination procedures based on those described above are established for each federal agency. Agencies need to ensure they have the capacity and processes in place to operate in challenging conditions. This includes dedicated leadership and availability of supporting personnel to manage additional operational demands, identification of relevant points of contact in other federal agencies and highlighting existing communications and decision-making processes essential for effective incident coordination. Security clearances should also be pre-approved to facilitate timely sharing of information.[66]

European Union

While the US NCIRP 2016 outlines an overall integrated approach to respond to significant cyber incidents, the EU Permanent Structure Cooperation (PESCO) project on 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security' offers a practical instrument to aid regional technical response to a significant cyber incident, operationalised through Cyber Rapid Response Teams (CRRTs). To date, eight EU countries – Belgium, Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania and Slovenia – have signed the memorandum of understanding for the project.[67]

According to a memo from the Lithuanian Ministry of National Defence,[68] the council of the participating member states is the main decision-making body of the CRRT. Following a cyber incident, the national institution with the highest authority for cyber issues in the affected member state would contact the chairman of the council for assistance in response measures. The request is submitted in the form of a standardised 'incident report' – which provides a description of the incident, the impact and the type of help required – which the chairman then shares among council members. Approval for activating the CRRT is granted unless there is an explicit objection. The decision-making process is limited to a reasonable timeframe to ensure a prompt response to the incident.

The memo does not specify the criteria required for cyber incidents to activate the CRRT, but recommends that member states refer to the EU Network and Information Security (NIS) Directive for guidance on establishing the threshold for a 'dangerous incident'.[69] Upon approval of the activation, the mission coordinator, which is the technical point of contact of the CRRT, assembles a team of experts with the requisite skills to manage the incident. The CRRT could comprise experts from each member state or from the member state leading the CRRT's rotation. Member-state representatives within the council need to be familiar with the technical expertise[70] available within their own country, both civilian and military. Security clearances for CRRT members should be obtained in advance to ensure access to sensitive information during their missions, suggesting private-sector expertise would most likely be unviable. The memo states that a non-disclosure agreement should be signed by the CRRT, while a liability waiver should be signed by the hosting member state to prevent the imposition of a liability on the CRRT for any unintended damage.

Besides the PESCO project, plans to establish an EU-wide framework for response to cyber emergencies are also underway. While the proposed framework is less mature than the US model, it offers a multinational solution that could inform an ASEAN framework for responding to cyber emergencies. The European Commission introduced Recommendation 2017/1584 on 'coordinated response to large-scale cyber security incidents or crisis' in 2017, in which the blueprint for coordinated response is laid out.[71] The blueprint dissects cooperation into three levels – technical, operational and strategic/political – at which activities concerning shared situational awareness, response and public communications are implemented. Coordination of response to a cyber-security emergency is led by the Presidency of the Council of the EU. The presidency activates an existing crisis-management mechanism such as the Integrated Political Crisis Response (IPCR) arrangement. Once the IPCR is activated, informal roundtable meetings gathering all stakeholders at member-state- and EU-level are held to support the presidency in handling the crisis. An Integrated Situational Awareness and Analysis report is drafted by either the

European Commission or the European External Action Service, along with all cyber-security stakeholders, to provide a strategic overview of the situation and support decision-making in the council. For major multi-sectoral crises that require action at the European level, the president of the European Commission would trigger Phase II of the ARGUS crisis-coordination process to enable real-time sharing of crisis-related information and rapid decision-making.[72]

While an official EU cyber-emergency-response plan has yet to be established, progress has been made towards implementing Recommendation 2017/1584. In 2019, an initiative by France and Spain established the table-top Blueprint Operational Level Exercise (Blue OLEx), which gathers together high-level national cyber-security authorities, the EU Agency for Cybersecurity (ENISA) and the European Commission in order to allow European states to deepen collaboration at the operational level by defining cooperation and exchange procedures during a cyber crisis.[73] In 2020, the Cyber Crisis Liaison Organisation Network (CyCLONe) was launched during the second iteration of Blue OLEx to act as an intermediary between the technical (EU Computer Security Incident Response Teams) and political (IPCR process) responses during a large-scale cyber-security incident or crisis. The network functions at the operational level by facilitating consultations on national response strategies and coordinating impact assessment among the appointed national cyber-security authorities and EU agencies.[74] Table-top exercises have since been held with officials and high-level actors in CyCLONe to test standard operating procedures and improve efficiency in collective cyber-emergency response.[75]

In June 2021 the EU Commission announced its plan to build the Joint Cyber Unit (JCU), a broad crisis-management platform that seeks to convene EU institutions, agencies and bodies, and authorities in member states, including civilian, law enforcement, diplomatic, cyber defence and private-sector partners, to prevent, deter and respond to large-scale cyber incidents and crises, while aiding member states to recover from such attacks.[76] The JCU aims to work on the operational and technical levels to ensure a coordinated EU response to large-scale cyber-security crises. Establishment of the JCU will follow a gradual process that aims for completion by June 2023. This process will first involve the delivery of an EU Cybersecurity Incident and Crisis Response Plan and the mobilisation of EU Cybersecurity Rapid Reaction Teams.[77]

Chapter Three: Limitations in ASEAN Cyber-cooperation Architecture

Lack of Regional Institutional Structures for Cyber-emergency Response

The US and EU incident-response models discussed in this report demonstrate the key elements of a cyber-emergency-response framework:

- an entity for overall decision-making in response to a cyber emergency;
- a platform or interconnected platforms engaging all cyber-security-related stakeholders to communicate, share information or coordinate activity;
- standard operating protocols for coordination; and
- defined roles and responsibilities for all cyber-security-related stakeholders.

In contrast, ASEAN's current cyber-cooperation architecture lacks a clear political authority and is loosely dispersed across various sectoral platforms. There is a clear need for a framework that connects all cyber-security communities in platforms spanning political-security, technical, economic and law enforcement[78] to support a coordinated response to cyber emergencies on both technical and operational levels. The recently established ASEAN Cybersecurity Coordinating Committee (Cyber-CC), though cross-sectoral in nature, only meets annually to promote policy coherence and align regional cyber-security policy with national operational considerations.

Lack of a Common Cyber Lexicon

Another factor hindering the establishment of a regional cyber-emergency-response capability is the lack of a common cyber lexicon defining the respective impacts of a significant cyber incident or cyber emergency on critical information infrastructure. For instance, Malaysia's National Security Council Directive No. 24 classifies cyber incidents into five levels. A cyber incident is classified as Level 4 if it results in 'widespread disruption or damage to CNII [critical national information infrastructure] agencies and/or organisations and results in significant impact on the country'; a Level 5 incident is declared a 'crisis' if it results in a 'critical impact on CNII agencies and/or organisations'.[79] However, neither 'widespread disruption or damage' nor 'critical impact' are defined.

In contrast, Vietnam outlines specific criteria of a 'serious cyber information-security incident' that warrant the activation of a national response. This would be triggered if the compromised information system[80] encounters problems such as disruption of service, compromised top-secret data or state secrets, damage to important data, or a large-scale attack that leads to cross-sectoral impacts.[81] Other countries in the region such as Cambodia and Indonesia have not yet defined a cyber emergency in similar terms to Malaysia and Vietnam.

Structural Obstacles Due to the Nature of ASEAN

A third obstructing factor is that, unlike the EU, which is a supranational entity, ASEAN's structure as an intergovernmental organisation poses challenges to formalising structures for collaboration in response efforts. Known as the 'ASEAN Way', member states cooperate based on the principles of respect of sovereignty, consensus-based decision-making and non-interference, which are enshrined in the 2007 ASEAN Charter. As a result, the ASEAN policy-making process is slow and its regional cyber policies are limited, lagging behind other regional bodies such as the EU.[82] For instance, while ASEAN member states highlighted the need to reduce the risk of misperception, escalation and conflict in the Statement on Cooperation in Ensuring Cyber Security in 2012, the Workplan on Security of and in the Use of ICTs was only developed three years later in 2015, and implementation was only possible after the establishment of the ARF ISM on ICT Security in 2017. Moreover, there is a general lack of trust given the diverse cultural and political context and history across the region, leading to limited sharing of threat intelligence.[83] For example, in the case of cyber crime, although ASEAN member states have achieved cooperation in practical ways, such

as conducting joint operations under the ASEAN Cyber Capability Desk, they have not agreed on an overarching regulation due to an overall disparity in cyber-crime laws and enforcement.[84]

Furthermore, due to the digital divide among ASEAN member states, the issue of a cyber-induced emergency may be a lower priority for developing countries like Cambodia, Laos and Myanmar, which are only beginning to develop their foundational ICT capabilities and digital economies.[85] ASEAN governments' views of cyber-space governance are also filtered through the lens of domestic political considerations. For instance, Singapore's Cybersecurity Act 2018 focuses on CIIP, while Vietnam's Law on Cybersecurity, passed in 2018, focuses on content control and data localisation.[86]

Shortage of Cyber-security Professionals

Another challenge that ASEAN states face in forming a regional emergency-response capability is the shortage of cyber-security professionals – a trend mirroring the global lack of cyber-security talent. This poses a challenge to technical cyber-response efforts, especially in forming a CRRT, which requires a wide variety of cyber-security skillsets.[87] The Philippines National CERT, for instance, only had 12 full-time employees in 2020.[88] Cambodia, Laos, Myanmar and Vietnam are in the early stages of cyber-security capacity building and are also struggling with a lack of resources and technical expertise. Even in the most digitally advanced countries in the region, such as Singapore and Malaysia, which have developed comprehensive strategies to nurture cyber-security talent,[89] there is still a severe shortage of cyber-security experts.[90] Not only is there a lack of human talent, but there is also an acute shortage of specific skillsets such as behavioural analytics and digital forensics.[91]

Uneven Development in Cyber-emergency-response Networks Across ASEAN

The development of multi-stakeholder networks for cyber-emergency response is uneven across ASEAN member states. Singapore and Malaysia have relatively well-developed national-emergency response networks that involve the private sector to a greater degree compared to other states in the region. Singapore has held three editions of *Exercise Cyber Star* since 2016, a nation-wide cyber crisis-management exercise involving multiple sector leads and CII owners to test their operational plans in response to complex simulated attacks.[92] As part of the 2019 Operational Technology (OT) Cybersecurity Masterplan, which aims to improve cross-sector response to cyber threats in the OT environment, the Cyber Security Agency of Singapore also partnered with the Global Resilience Foundation to establish the OT Cybersecurity Information Sharing and Analysis Center.[93] Similarly, Malaysia's *X-Maya National Cyber Crisis Exercise* simulates large-scale cyber attacks on CNII to help improve the National Cyber Security Response, Communication and Coordination Procedure, and test communications channels within CNII agencies, as well as between CNII agencies and their respective sector leads in government ministries.[94]

Countries such as Thailand and the Philippines have yet to formulate whole-of-nation emergency-response plans, but information-sharing networks between the government and the private sector have been established. For instance, Thailand's Electronic Transactions Development Agency (ETDA) shares cyber-threat intelligence with Cisco;[95] Vietnam's CERT entered into a strategic partnership in cyber-security-incident response with PricewaterhouseCoopers Vietnam in 2018; and the Philippines Air Force shares cyber-threat intelligence with PLDT.[96] Thailand and Vietnam, as well as Indonesia, have also signalled their intent to develop national incident-response plans that involve cooperation between the public and private sector.[97] However, for other countries in the region cyber-security development is still in its early stages[98] and they lack mechanisms for public–private partnership on cyber-security information sharing.

Chapter Four: Towards an ASEAN Cyber-emergency-response Framework

Designate a Political Authority and Establish a Common Platform

One of the key steps for ASEAN to establish a cyber-emergency-response framework is to designate a political authority for overall coordination in a cyber emergency. Given its cross-sectoral nature, the ASEAN Cybersecurity Coordinating Committee (Cyber-CC) could serve this role, which would be to approve the activation of emergency-response procedures once a cyber incident is designated a region-wide emergency, or when requested by a member state.

To ensure a coordinated response on an operational and technological level, ASEAN could establish a common platform akin to the Joint Cyber Unit (JCU) or the Cyber Unified Coordination Group (UCG), to bring together the expertise of cyber-related ASEAN cooperation groups,[99] including in technical, law enforcement, economics, politics, defence and the private sector. This platform could also interface with existing information-sharing networks such as the Asia Pacific Public Sector Cyber Security Executive Council by Microsoft,[100] the ASEAN Cyber Defence Network and the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) for central banks.

Adopt a Sector-based Approach

ASEAN could adopt a sector-based approach in its cyber-emergency-response plan, as seen in the US framework. In this approach, designated national authorities for each CII sector form information-sharing networks within their respective sectors, which in turn interface with the larger common platform like the JCU or the Cyber UCG. Information-sharing networks could first be established in priority CII sectors in each member state. For example, a recent study[101] conducted by Thailand's Electronic Transactions Development Agency on 'ASEAN Critical Information Infrastructure Protection' found that attacks on the transportation and ICT sectors are perceived to have the greatest cross-border impacts, while also being best placed for information sharing between member states. These information-sharing networks would help to assist swift coordination efforts during a cyber incident and allow early identification of a potential cyber emergency with cross-border impact across a CII sector.

For sectors deemed too sensitive for region-wide information sharing, ASEAN could adopt the 'ASEAN minus X' model, in which willing states could move ahead to collaborate, on the premise that other members would follow at a later stage.[102] Although this model was created primarily for economic matters, it has also been used for other cross-border threats.[103] These sector-specific networks could establish interfaces with global information-sharing frameworks, such as Information Sharing and Analysis Centers, to enable global collaboration.

Agree a Common Cyber Lexicon and Standard Operating Procedures

ASEAN should work to establish a common set of cyber terminology to ensure effective communication and information sharing during a cyber emergency.[104] For instance, member states could agree on the range of sectors to be considered as critical information infrastructure.

ASEAN also needs to set up standard operating procedures to enable effective and rapid communication and information sharing. The first step is to agree on a common schema for cyber-incident classification and the types of response activities involved in each level, such as agreeing on a definition of a cyber emergency and when cyber-emergency procedures should be triggered. Response actions could then be determined and categorised, for example following the model of the United States' National Cyber Incident Response Plan (threat response, asset response and intelligence support), with clear roles and responsibilities assigned for each stakeholder.

To facilitate coordination, directories of points-of-contact (POCs) in technical, security, policy, law-enforcement and defence cyber agencies should be

created and regularly updated. This could leverage similar work done by the ASEAN Regional Forum Inter-Sessional Meeting on ICTs Security (ARF ISM on ICTs Security) and ASEAN Defence Ministers' Meeting-Plus Cyber Security Expert Working Group (ADMM-Plus CS EWG).[105] Secure channels of communication and backup systems should also be pre-determined to enable sharing of confidential information. In some ASEAN countries, new legislation will be needed to enable cross-border threat investigation or threat mitigation in a cyber emergency.[106]

Develop Deployable Operational Capability for Mutual Assistance

Part of ASEAN's coordinated response effort could involve developing a deployable operational capability in the form of a Cyber Rapid Response Team (CRRT), as exemplified in the EU's Permanent Structure Cooperation (PESCO) project, to facilitate responding to requests for assistance by member states. ASEAN members already have experience deploying ASEAN Emergency Response and Assessment Teams (ASEAN-ERAT), which assemble relevant expertise for managing natural disasters.[107] In the same way, CRRTs could draw relevant experts from every member state, from both military and civilian units, and be deployed to the affected state and/or the state from which the threat is emanating. Given the capability gap among member states,[108] ASEAN countries could contribute to the CRRT in proportion to their respective human-resource capacities. Sustained investments in regional cyber capacity-building initiatives such as the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) will be crucial to bridge capability gaps.

Standard operating procedures should be established to facilitate member states' requests for assistance and ASEAN responses to such requests. For instance, ASEAN could follow a common template for assistance requests which include standardised elements such as acknowledgement and approval of request, timeframe, nature, scope and terms of assistance to be provided.[109] This would help to ensure critical information is conveyed in an efficient and timely fashion.

Conclusion

ASEAN has seen much progress in improving its institutional framework to address cyber threats. Not only has it strengthened its regional platforms for discussion of cyber-security issues, but it has also improved the region's overall cyber-security preparedness through information sharing across various sectoral bodies and capacity-building projects. Cyber security is no longer viewed as a technical issue involving national Computer Emergency Response Teams (CERTs) but a multidisciplinary issue straddling the political, economic, defence and law-enforcement domains. While efforts have been made to strengthen cross-sectoral regional coordination on cyber security, such as via the establishment of ASEAN Cybersecurity Coordinating Committee (Cyber-CC) in 2019, progress to date has been limited and regional cyber-cooperation architecture remains largely dispersed. Crucially, ASEAN does not possess a regional mechanism for responding to cyber emergencies or requests for assistance in a cyber emergency. Building such a mechanism is increasingly vital given the escalating risks to CII in the region that originate from accelerating digitalisation, escalating cyber crime or unfavourable geopolitical factors.

Using models from the US and EU contexts, this report has attempted to demonstrate how ASEAN could develop a cyber-emergency-response framework by establishing relevant institutions and procedures to facilitate political, technical and operational coordination. The report recommended establishing a deployable CRRT to help strengthen cyber resilience in the region, given uneven development in cyber-security and IT capabilities among ASEAN member states. ASEAN need not reinvent the wheel but rather could adapt existing approaches developed by the EU and US to build a cyber-emergency-response capability to suit the region's needs.

ASEAN can leverage its experience establishing a regional response mechanism for traditional crises to build a similar framework for cyber emergencies. This requires a greater degree of investment and political will, given the varying levels of digitalisation and security priorities among member states. Nevertheless, in the face of intensifying numbers of cyber attacks on national and cross-border CII within ASEAN, developing a regional cyber-emergency-response framework is both a timely endeavour to address current challenges, and an important step towards future operationalisation of UN-recommended norms.

Notes

1 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', United Nations General Assembly, 22 July 2015, p. 8, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

2 In this report, a 'cyber incident' can broadly be defined as a breach in a computer system aimed at compromising the integrity, availability or confidentiality of its data or that of other systems connected to it. This definition is adapted from definitions used in the US, UK and EU contexts. See The White House, 'Presidential Policy Directive – United States Cyber Incident Coordination', 26 July 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident; National Cyber Security Centre, 'What Is a Cyber Incident', https://www.ncsc.gov.uk/information/what-cyber-incident; Official Journal of the European Union, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union', 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

3 The five levels from 1 to 5 are 'Low', 'Medium', 'High', 'Severe' and 'Emergency'. US Department of Homeland Security, 'National Cyber Incident Response Plan', December 2016, p. 39, https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf. The UK, similar to the US, classifies national cyber incidents into different categories based on severity. These range from 1 to 6: 'Localised incident', 'Moderate incident', 'Substantial incident', 'Significant incident', 'Highly significant incident' and 'National cyber emergency'. See National Cyber Security Centre, 'New Cyber Attack Categorisation System to Improve UK Response to Incidents', 11 April 2018, https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.

4 US Department of Homeland Security, 'National Cyber Incident Response Plan'.

5 A cyber-security incident considered as a 'crisis' at the EU level is also referred to as a 'large-scale cybersecurity incident'. See Official Journal of the European Union, 'Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-scale Cybersecurity Incidents and Crises', 19 September 2017, p. 36, https://eur-lex.europa.eu/eli/reco/2017/1584/oj/eng.

6 OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy, 'OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]', June 2008, p. 4, https://www.oecd.org/sti/40825404.pdf.

7 'Ransomware Attacks Nation's Largest Cancer Hospital', The Jakarta Post, 15 May 2017, https://www.thejakartapost.com/news/2017/05/15/ransomware-attacks-nations-largest-cancer-hospital.html.

8 'Southeast Asia: An Evolving Cyber Threat Landscape', Fireeye Threat Intelligence, March 2015, p. 3, https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/rpt-southeast-asia-threat-landscape.pdf; Windows Defender Advanced Threat Hunting Team, 'Platinum: Targeted attacks in South and Southeast Asia', Microsoft, 29 April 2016, p. 4, https://www.microsoft.com/en-us/download/details.aspx?id=51956.

9 Supervisory Control and Data Acquisition (SCADA) systems help to manage industrial control systems by providing a graphical user interface that displays the process under control and provides access to control functions. See KuppingerCole, 'OT, ICS, SCADA – What's the Difference?', 7 July 2015, https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

10 Akshaya Asokan, 'Hackers Target Critical Infrastructure in Southeast Asia', 7 August 2021, BankInfoSecurity, https://www.bankinfosecurity.com/hackers-target-critical-infrastructure-in-south-east-asia-a-17237.

11 Mark Lechtik and Giampaolo Dedola, 'Cycldek: Bridging the (air) gap', 3 June 2020, Securelist by Kaspersky, https://securelist.com/cycldek-bridging-the-air-gap/97157/; Anthony Eich, 'Advanced Persistent Threat "Naikon" Deploys New Malware', 29 April 2021, University of Hwai'i-West O'ahu, https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/advanced-persistent-threat-naikon-deploys-new-malware/.

12 Even with physical isolation, the Stuxnet incident, which destroyed numerous nuclear centrifuges in Iran's uranium-enrichment facility, has proven that such air gap controls can be bypassed through the insertion of an infected USB flash drive. See Kim Zetter, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', Wired, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

13 Industry 4.0, otherwise known as the Fourth Industrial Revolution, can be understood as the 'marriage of physical assets and advanced digital technologies – the Internet of Things, artificial intelligence, robots, drones, autonomous vehicles, 3D printing, cloud computing, nanotechnology, and more – that communicate, analyse, and act upon information, enabling organizations, consumers, and society to be more flexible and responsive and make more intelligent, data-driven decisions.' See: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/human-capital/Deloitte_Review_26_Fourth_Industrial_Revolution.pdf, p. 3.

14 ASEAN Connectivity consists of three aspects – physical, institutional and people-to-people. The strategies include developing ICT-related infrastructure for digital innovation, supporting ICT solutions for logistics growth, and developing aviation, road, rail and maritime links. See ASEAN Secretariat, 'Master Plan on ASEAN Connectivity 2025', August 2016, p. 41, https://asean.org/wp-content/uploads/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf; ASEAN Connectivity microsite, 'National Efforts Related to ASEAN Connectivity', 12 May 2020, https://connectivity.asean.org/resource/cross-border-connectivity-regional-needs-and-the-role-of-infrastructure-asia/.

15 Frederic Petit et al., 'Analysis of Critical Infrastructure Dependencies and Interdependencies', Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory, June 2015, https://publications.anl.gov/anlpubs/2015/06/111906.pdf; Kamonphorn Kanchana, Benjamin C. McLellan, and Hironobu Unesaki, 'Energy Dependence with an Asian Twist? Examining International Energy Relations in Southeast Asia', *Energy Research & Social Science*, vol. 21, November 2016, pp. 123–140, https://doi.org/10.1016/j.erss.2016.07.003.

16 Top cyber-security threats in ASEAN include business email compromise, phishing, ransomware, e-commerce data interception, crimeware-as-a-service, cyber scams and cryptojacking. These trends were ongoing prior to COVID-19. See INTERPOL, 'INTERPOL Report Charts Top Cyberthreats in Southeast Asia', 22 January 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia.

17 Joe Devanesan, '70% of SEA Population Are Targets for Cyber Criminals', Techwire Asia, 15 January 2021, https://techwireasia.com/2021/01/70-of-sea-population-are-targets-for-cyber-criminals/.

18 A cyber attack on Singapore's logistics and supply chain, for instance, would result in cascading disruption in services, given its status as a global trading hub. 'Building Cyber Security into Critical Infrastructure – Protecting Industrial Control Systems in Asia Pacific', Deloitte, 2020, p. 8, https://www2.deloitte.com/sg/en/pages/risk/articles/building-cyber-security.html.

19 INTERPOL, 'ASEAN Cyberthreat Assessment 2021 – Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk', 27 May 2021, p. 12, https://sitic.org/asean-cyberthreat-assessment-2021/.

20 Kenny Chee, 'Nearly 73,500 Patients' Data Affected in Ransomware Attack on Eye Clinic in S'pore', Straits Times, 26 August 2021, https://www.straitstimes.com/tech/tech-news/nearly-73500-patients-data-affected-in-ransomware-attack-on-eye-clinic-in-spore; 'Axa Division in Asia Hit by Ransomware Cyber Attack', Reuters, 16 May 2021, https://www.reuters.com/article/us-axa-cyber-idUSKCN2CX0B0.

21 The ASEAN Information Infrastructure is only a collection of national assets. See Association of Southeast Asian Nations, 'e-ASEAN Framework Agreement', 24 November 2000, p.4, http://agreement.asean.org/media/download/20140119121135.pdf.

22 Infocomm Media Development Authority, 'ICT Ministers Advance Efforts to Build a Secure Cyberspace and Promote Trade in Telecommunications Equipment', 19 September 2003, https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2003/20061107180752.

23 Caitríona H. Heinl, 'Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime', Asia Policy, no. 18, 21 July 2014, p. 159, https://www.nbr.org/publication/regional-cybersecurity-moving-toward-a-resilient-asean-cybersecurity-regime/.

24 Association of Southeast Asian Nations, 'Brunei Action Plan "Enhancing ICT Competitiveness: Capacity Building"', 19 September 2006, https://asean.org/brunei-action-plan-enhancing-ict-competitiveness-capacity-building/.

25 Association of Southeast Asian Nations, 'ASEAN ICT Masterplan 2015 Completion Report', December 2015, p. 25, https://asean.org/wp-content/uploads/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf. Even before ANSAC, the ASEAN Telecommunication Regulators' Council (ATRC) – a committee focused on regional technical regulatory issues – had established the Framework for Cooperation in Network Security in 2005. See International Telecommunication

Union 'The ASEAN Telecommunication Union Regulators' Council (ATRC) Work Plan 2005–2006', https://www.itu.int/ITU-D/treg/Events/Seminars/2005/RegRegAssoc/ATRC%20Workplan%202005.pdf.

26 The ASEAN CERT Maturity Framework is an outcome of the Cybersecurity Cooperation Strategy, which was approved at the 16th TELMIN in 2016, focusing on three main areas of incident response: policy building and coordination among national CERTs, and cyber-security capacity building. The framework addresses the challenge of CERT coordination due to the varying levels in capability by providing a common blueprint that enables national CERTs to self-assess their maturity levels. See Brad Glosserman, 'ARF to the Forefront: Promoting Cybersecurity CBMs in the Asia-Pacific', *Issues & Insights*, vol. 17, no. 7, May 2017, p. 4, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/PacificForum-issuesinsights_vol17no7.pdf; Association of Southeast Asian Nations, 'The 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings', 26 November 2016, p.1, https://asean.org/wp-content/uploads/2021/03/69.pdf; Cyber Security Agency of Singapore, 'Opening Remarks by Mr S Iswaran, Minister for Communications and Information, at The ASEAN Ministerial Conference on Cybersecurity', 19 September 2018, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/9/opening-remarks-by-mr-s-iswaran-at-the-asean-ministerial-conference-on-cybersecurity?page=234_6.

27 There is, however, a lack of transparency surrounding the outcomes of these projects. For instance, the feasibility study for establishing an ASEAN CERT and the Incident Reporting Framework were not published. See Association of Southeast Asian Nations, 'Final Review - ASEAN ICT Masterplan 2020', 2020, p. 64, https://asean.org/wp-content/uploads/2021/02/V4.-Final-Draft-_-AIM2020_Review_FInal_Draft_19Nov2020.pdf.

28 100% of respondents thought the feasibility study for establishing an ASEAN CERT and the Incident Reporting Framework produced valuable results, compared to nearly 67% of respondents who thought developing an ASEAN framework on personal data protection produced valuable or highly valuable results. *Ibid*., pp. 63–64.

29 Association of Southeast Asian Nations, 'ASEAN Digital Masterplan 2025', 2021, p. 22, https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf.

30 Singapore Ministry of Communications and Information, '1st ASEAN Digital Ministers' Meeting Approves Singapore-led Initiatives on ASEAN Data Management Framework, ASEAN Model Contractual Clauses for Cross Border Data Flows and ASEAN CERT Information Exchange Mechanism', 22 January 2021, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/1/1st-asean-digital-ministers-meeting.

31 Cyber Security Agency of Singapore, 'Establishment of ASEAN Regional Computer Emergency Response Team (CERT)', 20 October 2022, https://www.csa.gov.sg/News-Events/Press-Releases/2022/establishment-of-asean-regional-computer-emergency-response-team#:~:text=The%20ASEAN%20Regional%20CERT%20is,and%20the%20Financing%20Model%20thereafter.

32 Platforms working to achieve the third pillar of ASEAN cooperation – socio-cultural cooperation – deal with content-related issues of cyberspace. For instance, the ASEAN Ministers Responsible for Information adopted a joint statement in September 2020 to combat fake news and misinformation surrounding the COVID-19 pandemic. See http://www.aseanthai.net/english/ewt_news.php?nid=3556&filename=index_2.

33 Chairman's Statement of the 24th ASEAN Regional Forum, 'Partnering for Change, Engaging the World', 7 August 2017, p. 6, https://asean.org/wp-content/uploads/2017/08/Chairmans-Statement-of-the-24th-ARF-FINAL.pdf.

34 Also known as the Coordinating Committee on Cybersecurity in the 2019 TELMIN Joint Media Statement. See Association of Southeast Asian Nations, 'Joint Media Statement of the 19th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings', 25 October 2019, p. 2, https://asean.org/wp-content/uploads/2021/09/ADOPTED-TELMIN-19th-TELMIN-JMS-.pdf.

35 Cyber Security Agency of Singapore, 'ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism', 2 October 2019, https://www.csa.gov.sg/News-Events/Press-Releases/2019/AMCC-Release-2019.

36 ASEAN Secretariat, 'ASEAN Economic Community Blueprint 2025', 2015, p. 23, https://asean.org/wp-content/uploads/2021/08/AECBP_2025r_FINAL.pdf.

37 ASEAN Secretariat, 'The ASEAN ICT Masterplan 2020', 2015, p. 26, https://www.aseanrokfund.com/resources/the-asean-ict-masterplan-2020.

38 Association of Southeast Asian Nations, 'ASEAN Leaders' Statement on Cybersecurity Cooperation', 27 April 2018, p.3, https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf.

39 *Ibid*.

40 Singapore Ministry of Communications and Information, 'ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-building Efforts', 19 September 2018, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/9/asean-members-states-agree-to-strengthen-cyber-coordination-and-capacity-building-efforts.

41 Cyber Security Agency of Singapore, 'ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism'.

42 Singapore Ministry of Communications and Information, 'Keynote Address by Mrs Josephine Teo, Minister for Communications and Information, at ASEAN Ministerial Conference on Cybersecurity on 6 Oct 2021', 6 October 2021, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/10/keynote-address-by-mrs-josephine-teo-at-asean-ministerial-conference-on-cybersecurity.

43 Association of Southeast Asian Nations and Electronic Transactions Development Agency, 'ASEAN Critical Information Infrastructure Protection Framework', pp. 7–9, 2020, https://www.etda.or.th/th/Useful-Resource/publications/ASEAN-Critical-Information-Infrastructure-Protection-Framework.aspx.

44 The ASCCE also covers cyber policy, and technical and operational training for AMS. It maximises resources via engaging dialogue partners, private-sector experts, international organisations and academia. See Cyber Security Agency of Singapore, 'ASEAN-Singapore Cybersecurity Centre of Excellence', 6 October 2021, https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence.

45 Cybil, 'Annual CIIP Workshops in ASEAN', https://cybilportal.org/projects/annual-ciip-workshops-in-asean/; Cybil, 'Annual Cyber Exercises in ASEAN', Cybil, https://cybilportal.org/projects/annual-cyber-exercises-in-asean/.

46 'Vietnam Hosts 2018 ASEAN-Japan Cyber Security', *NhânDân*, 23 May 2018, https://en.nhandan.vn/scitech/sci-tech/item/6190102-vietnam-hosts-2018-asean-japan-cyber-security.html.

47 Association of Southeast Asian Nations, CIIP Guidelines Ver 3.0', The 9th ASEAN-Japan Information Security Policy Meeting, 20 October 2016, https://asean.org/wp-content/uploads/2012/05/01-CIIP-Guidelines-Ver3.0.pdf.

48 EU-Japan Centre for Industrial Cooperation, 'Japanese Industry and Policy News', September 2018, https://eu-japan.eu/sites/default/files/publications/docs/japanese_industry_and_policy_news_september_2018.pdf; Government of Japan, 'Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region Held', 12 September 2019, https://www.japan.go.jp/publications/news/2019-09-21_432.html; Japanese Ministry of Economy, Trade and Industry, 'Japan – US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region in FY2020', 15 March 2021, https://www.meti.go.jp/english/press/2021/0315_001.html.

49 Yukio Tajima, 'Japan to Lead First Cyber Defense Drill with ASEAN, US and Europe', Nikkei Asia, 9 August 2020, https://asia.nikkei.com/Business/Technology/Japan-to-lead-first-cyber-defense-drill-with-ASEAN-US-and-Europe.

50 ASEAN Regional Forum, 'Co-Chairs' Minutes: 5th ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies', 16 January 2020, https://aseanregionalforum.asean.org/wp-content/uploads/2021/01/Co-chairs-Minutes-5th-ARF-OESG.pdf.

51 Monetary Authority of Singapore, 'Joint Statement of the 7th ASEAN Finance Ministers and Central Bank Governors' Meeting (AFMGM)', 31 March 2021, https://www.mas.gov.sg/news/media-releases/2021/joint-statement-of-the-7th-asean-finance-ministers-and-central-bank-governors-meeting; Bank Negara Malaysia, 'Annual report 19', 31 Mar 2020, p. 70, https://www.bnm.gov.my/documents/20124/2724769/ar2019_en_full.pdf.

52 ASEAN Regional Forum, 'Chairman's Statement of the 28th ASEAN Regional Forum', 6 August 2021, p. 6, https://www.mofa.go.jp/files/100220807.pdf.

53 Singapore Ministry of Defence, '15th Anniversary of ADMM: Preparing for a Future-Ready, Peaceful and Prosperous ASEAN', 15 June 2021, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/June/15jun21_nr.

54 'Concept Paper on the Establishment of ASEAN Cyber Defence Network (ACDN)', as adopted by the 15th ADMM, 15 June 2021, https://admm.asean.org/dmdocuments/2021_Jun_15th%20ADMM_15%20June%202021,%20VC_7.%20Concept%20Paper%20on%20the%20ASEAN%20Cyber%20Defence%20Network%20(ACDN)%20[Malaysia].pdf.

55 'Concept Paper on ADMM Cybersecurity and Information Centre of Excellence', as adopted by the 15th ADMM, 15 June 2021, https://admm.asean.org/dmdocuments/2021_Jun_15th%20ADMM_15%20June%202021,%20VC_5.%20Concept%20Paper%20on%20the%20ADMM%20Cybersecurity%20and%20Information%20Centre%20of%20Excellence%20[Singapore].pdf.

56 ASEAN Regional Forum, '15th ASEAN Regional Forum Inter-Sessional Meeting on Counter-Terrorism and Transnational Crime', 6 –7 April 2017, p. 8, https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/Report-15th-ARF-ISM-CTTC-CLEAN.pdf; CSCAP is also holding study group meetings regarding International Law and Cyberspace which would contribute to discussions at the ARF ISM on ICT Security. See Council for Security Cooperation in the Asia Pacific, '1st Meeting of the CSCAP Study Group on International Law and Cyberspace', 2019, http://www.cscap.org/uploads/CSCAP%20Co-chairs%20Report%20for%20First%20Study%20Group%20.pdf.

57 ASEAN's principles of respect of sovereignty and non-interference in internal affairs have always underlined most member states' preference for a national rather than a multi-stakeholder approach in governance. However, the 2018 Leaders' Statement on Cybersecurity Cooperation demonstrates that ASEAN states recognise the 'value of enhanced dialogue and cooperation on cybersecurity issues with Dialogue Partners and other External Parties'. See 'ASEAN Leaders' Statement on Cybersecurity Cooperation', 32nd Association of Southeast Asian Nations, 27 April 2018, p. 3, https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/.

58 Monetary Authority of Singapore and Financial Services Information Sharing and Analysis Center, 'FS-ISAC and MAS Establish Asia Pacific (APAC) Intelligence Centre for Sharing And Analysing Cyber Threat Information', 1 December 2016, https://www.mas.gov.sg/news/media-releases/2016/fs-isac-and-mas-establish-apac-intelligence-centre; Monetary Authority of Singapore, 'FS-ISAC and MAS to Strengthen Cyber Information Sharing Across Nine Countries', 14 November 2017, https://www.mas.gov.sg/news/media-releases/2017/fs-isac-and-mas-to-strengthen-cyber-information-sharing-across-nine-countries.

59 'Cybersecurity in ASEAN: An Urgent Call to Action', AT Kearney, 2018, p. 1, https://www.kearney.com/documents/20152/989824/Cybersecurity+in+ASEAN.pdf/2e0fb55c-8a50-b1e3-4954-2c5c573dd121.

60 US Department of Homeland Security, 'National Cyber Incident Response Plan', p. 4.

61 US Department of Homeland Security, 'National Cyber Incident Response Plan', p. 33.

62 Presidential Policy Directive 21 identified 16 critical infrastructure sectors – chemical, commercial facilities, communications, critical manufacturing, dams, defence-industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. The White House, 'Presidential Policy Directive -- Critical Infrastructure Security and Resilience', 12 February 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

63 Each GCC acts as a counterpart to each SCC and is made up of various government agencies that enable interagency and interjurisdictional coordination. Each GCC is led by an SSA, which engages in information sharing, coordination, incident response and technical assistance responsibilities within its assigned sector and in cross-sector security and resilience efforts.

64 See Center for Internet Security, 'Multi-State Information Sharing and Analysis Center (MS-ISAC)', www.cisecurity.org/ms-isac/.

65 See National Council of Isacs, 'About NCI', https://www.nationalisacs.org/about-nci.

66 US Department of Homeland Security, 'National Cyber Incident Response Plan', p. 49.

67 Lithuanian Ministry of Defence, 'Lithuanian-coordinated EU Cyber Rapid Response Teams – Incident Response with the EU and in Support of EU Partners and Military Missions', 30 March 2023, https://kam.lt/en/lithuanian-coordinated-eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/.

68 Egle Vasiliauskaite and Tadas Sakunas, 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security – Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs' Operations, Lessons Learnt from the Cyber Shield/ Amber Mist 2018 Exercise', Cyber Security and Information Technology Department, Ministry of National Defence of the Republic of Lithuania, 2018, https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf.

69 Ibid., p. 18. See also Official Journal of the European Union, 'Directive (EU) of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)', 27 December 2022, p. 112, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN.

70 Technical expertise required in a CRRT may include malware analysis, network forensics, intrusion detection and knowledge of an information communications system from a particular manufacturer.

71 Official Journal of the European Union, 'Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-scale Cybersecurity Incidents and Crises', 19 September 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN.

72 Phase II of ARGUS involves convening emergency meetings of the Crisis Coordination Committee, made up of representatives of relevant commission directorate generals, cabinets and other EU services. The Crisis Coordination Committee performs situational assessment, decides on the response measures and ensures they are being implemented. *Ibid*., p. 53.

73 National Cybersecurity Agency of France, 'Blue Olex 2019: Member States' New Initiative to Develop the European Cyber Crisis Management System', NIS Cooperation Group, 1 July 2019, https://www.ssi.gouv.fr/uploads/2019/07/press-release-blue-olex-2019.pdf.

74 European Union Agency for Cybersecurity, 'Blue OLEx 2020: the European Union Member States Launch the Cyber Crisis Liaison Organisation Network (CyCLONe)', 29 September 2020, https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

75 European Union Agency for Cybersecurity, 'EU Member States Test Rapid Cyber Crisis Management', 19 May 2021, https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management; European Union Agency for Cybersecurity, 'Blue OLEx 2021: Testing the Response to Large Cyber Incidents', 12 October 2021, https://www.enisa.europa.eu/news/blue-olex-2021-testing-the-response-to-large-cyber-incidents; European Union Agency for Cybersecurity, 'Blue OLEx 2022 Tests the Standard Operating Procedures of the EU CyCLONe', 7 November 2022, https://www.enisa.europa.eu/news/blue-olex-2022-tests-the-standard-operating-procedures-of-the-eu-cyclone.

76 European Commission, 'Joint Cyber Unit', last updated 7 June 2022, https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit. The EU cyber-security community includes the EU Agency for Cybersecurity (ENISA); Cybersecurity National Authorities; technical groups such as National CSIRTs, CERT-EU; coordinating networks such as the Cyber Crisis Liaison Organisation Network (CyCLONe) and the Horizontal Working Party on Cyber Issues; law-enforcement agencies such as Europol's European Cybercrime Centre; defence cyber groups such as the European Defence Agency and PESCO; and cyber-diplomacy groups such as the European Foreign Affairs Council and the European External Action Service.

77 European Commission, 'Factsheet: Joint Cyber Unit', 18 June 2021, https://digital-strategy.ec.europa.eu/en/library/factsheet-joint-cyber-unit; Official Journal of the European Union, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)', 27 December 2022, p. 117, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN.

78 Political-security platforms include the ASEAN Defence Ministers Meeting-Plus Cyber Security Expert Working Group (ADMM-Plus CS EWG) and the ASEAN Regional Forum Inter-sessional Meeting on ICTs Security (ARF ISM on ICTs Security). Technical, economic and law-enforcement platforms include the ASEAN Regional Computer Emergency Response Team (CERT), the ASEAN Digital Ministers' Meeting (ADGMIN), and the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), respectively.

79 Malaysia National Security Council, 'Arahan Mkn No. 24: Dasar & Mekanisme Pengurusan Krisis Siber Negara' [MKN Directive No. 24: National Security Council National Cyber Crisis Management Policy & Mechanism], 2013, p. 29, http://marine21.marine.gov.my/appl/JPICT/JPICT012019/AGENDA%20104%20Arahan%20MKN%20No.%2024%20-%20MOT%20FINAL.pdf; Malaysia National Cyber Security Agency, 'National Security Council's Directive No. 24', https://www.cybersecurity.my/data/content_files/44/1212.pdf?.diff=1385607561.

80 The compromised information system here refers to Grade-4 and Grade-5 information systems, as defined in the National Decree 85/2016/ND-CP on the Security of Information Systems by Classification or those on the 'List of important information systems' in the Cyber Security Law 2018. See Government of the Socialist Republic of Vietnam, 'Decree on the Security of Information Systems by Classification', 1 July 2016, No. 85/2016/ND-CP, https://vanbanphapluat.co/decree-85-2016-nd-cp-on-the-security-of-information-systems-by-classification; National Assembly of the Socialist Republic of Vietnam, 'Law on Cybersecurity', No. 24/2018/QH14, 12 June 2018, https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-164904-d1.html.

81 Prime Minister Nguyen Xuan Phuc, Government of the Socialist Republic of Vietnam, 'Decision Providing for Emergency Response Plans to Ensure National Cyberinformation Security', No. 05/2017/QD-TTg, 16 March 2017, https://vanbanphapluat.co/decision-05-2017-qd-ttg-providing-emergency-response-plans-ensure-national-cyberinformation-security. For an important update in 2022, see also Government of Vietnam, 'Prime Minister Orders Strengthening Response to Cyber Information Security Incidents', 13 October 2022, https://en.baochinhphu.vn/prime-minister-orders-strengthening-response-to-cyberinformation-security-incidents-11122101415331275 3.htm.

82 Sharmaine Marmita, 'Struggle of ASEAN in Cyber Security', *Asia and Africa*, Issue 8, 8 September 2020, https://asaf-today.ru/s032150750010451-8-1/?sl=en.

83 George Christou and Michael Raska, 'Cybersecurity', in Thomas Christiansen, Emil Kirchner, and See Seng Tan (eds.), *The European Union's Security Relations with Asian Partners* (Cham: Palgrave Macmillan, 2021), pp. 213, https://doi.org/10.1007/978-3-030-69966-6_10.

84 Eugenio Benincasa, 'ASEAN Needs to Enhance Cross-border Cooperation on Cybercrime', The Strategist, Australian Strategic Policy Institute, 19 January 2021, https://www.aspistrategist.org.au/asean-needs-to-enhance-cross-border-cooperation-on-cybercrime/; Nathalie Van Raemdonck, 'Cyber Diplomacy in Southeast Asia', Digital Dialogue, EU Cyber Direct, May 2021, p. 23, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/2ZycxfN1/dd-southeast-asia-nb-fb-nvr-09-05.pdf.

85 'Can ASEAN Continue to Improve Cybersecurity in the Region and Beyond?', Council on Foreign Relations, 22 March, 2018, https://www.cfr.org/blog/can-asean-continue-improve-cybersecurity-region-and-beyond; Ratha Lim and Kunvath Sok, 'Sub-regional Views on International Cybersecurity: CLMV Countries', in Eneken Tikk and Mika Kerttunen (eds.), *Routledge Handbook of International Cybersecurity* (London: Routledge, 2020), p. 232, https://www.taylorfrancis.com/chapters/edit/10.4324/9781351038904-22/sub-regional-views-international-cybersecurity-ratha-lim-kunvath-sok.

86 Gisela Elsner and Aishwarya Natarajan, Regulating the Cyberspace: Perspectives from Asia, Konrad Adenauer Stiftung, 2020, p. 27, https://www.kas.de/documents/278334/8513721/Regulating+The+Cyberspace.pdf/c38a66be-6f35-45b9-73b3-273b4b55ebbd?version=1.0&t=1598321105440.

87 The skillsets required in a CRRT cover areas including malware, network forensics, network general monitoring, infrastructure, industrial control system and intrusion detection systems. See Vasiliauskaite and Sakunas, 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security – Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs' Operations, Lessons Learnt from the Cyber Shield/Amber Mist 2018 Exercise', p. 24.

88 APCERT Secretariat, 'APCERT Annual Report 2020', 2020, p. 89, https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf.

89 'Cybersecurity in ASEAN: An Urgent Call to Action', ATKearney, p. 12.

90 Sandhya Menon, 'CyberSecurity Malaysia: We Need More Experts', Star, 19 September 2021, https://www.thestar.com.my/news/education/2021/09/19/cybersecurity-malaysia-we-need-more-experts; 'A Different Pandemic in Cyberspace – And a Shortage of Front Liners', National University of Singapore Institute of Systems Science, 12 June 2020, https://www.iss.nus.edu.sg/community/newsroom/news-detail/2020/06/12/a-different-pandemic-in-the-cyberspace-and-a-shortage-of-front-liners.

91 'Cybersecurity in ASEAN: An Urgent Call to Action', ATKearney, p. 12.

92 Cyber Security Agency of Singapore, '11 CII Sectors Tested on More Complex Cyber Attack Scenarios', 4 September 2019, https://www.csa.gov.sg/News-Events/Press-Releases/2019/Exercise-Cyber-Star-2019; Cyber Security Agency of Singapore, 'CSA Marks Operational Milestone with Exercise Cyber Star', 22 March 2016, https://www.nas.gov.sg/archivesonline/data/pdfdoc/20160322001/160322_Press%20release_Cyber%20Star.pdf.

93 Cyber Security ASEAN, 'OT-ISAC Launched to Reduce Cybersecurity Risks to Operational Technology Critical Information Infrastructure in Singapore', 1 October 2019, https://cybersecurityasean.com/news-press-releases/ot-isac-launched-reduce-cybersecurity-risks-operational-technology-critical/.

94 Prime Minister's Department, Malaysia National Security Council, 'Malaysia Cyber Security Strategy 2020-2024', 2020, p. 10, https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf.

95 '4 Draft Digital Laws Ready for Cabinet as Govt Boosts Cybersecurity', *The Nation Thailand*, 2 September 2018, https://www.nationthailand.com/tech/30353553.

96 PLDT was previously known as the Philippine Long Distance Telecommunications Company. On the strategic partnership with PwC Vietnam, see Mark Manantan, 'The Promise of Public-private Cybersecurity Partnerships in the Philippines', EastAsia Forum, 21 October 2020, https://www.eastasiaforum.org/2020/10/21/the-promise-of-public-private-cybersecurity-partnerships-in-the-philippines/.

97 Cybersecurity Act B.E. 2562 (2019), Government Gazette No. 136 Chapter 69 Kor (Unofficial Translation), 27 May 2019, p. 12, https://www.cc.kmutt.ac.th/Files/cybersecrutiy-act-2019-en.pdf; Prime Minister of the Independent Socialist Republic of Vietnam, 'Phê Duyệt Đề Án Đẩy Mạnh Hoạt Động Của Mạng Lưới Ứng Cứu Sự Cố, Tăng Cường Năng Lực Cho Các Cán Bộ, Bộ Phận Chuyên Trách Ứng Cứu Sự Cố An Toàn Thông Tin Mạng Trên Toàn Quốc Đến 2020, Định Hướng Đến 2025' [Decision 1622/QD-TTG in 2017 on Approving the Project to Promote the Activities of the Incident Response Network, Strengthen the Capacity of Officials and Departments Specialised in Responding to Cyberinformation Security Incidents Nationwide Until 2020, Oriented to 2025], 25 October 2017, https://bachkhoaluat.vn/van-ban-luat/13656/quyet-dinh-1622-qdttg-nam-2017-ve-phe-duyet-de-an-day-manh-hoat-dong-cua-mang-luoi-ung-cuu-su-co-tang; Greta Nabbs-Keller, RM Eibawanto Nugroho Widodo, 'Indonesia Responds to the Cyber Dark Side', The Interpreter, 13 May 2021, https://www.lowyinstitute.org/the-interpreter/indonesia-responds-cyber-dark-side.

98 'Cybersecurity in ASEAN: An Urgent Call to Action', ATKearney, p. 51.

99 Such as the ADMM, AMCC, AMMTC, ARM ISM on ICTs Security and ADMM-Plus CS EWG.

100 Microsoft, 'Microsoft Launches First Asia Pacific Public Sector Cyber Security Executive Council Across Seven Markets tn the Region', 31 May 2021, https://news.microsoft.com/en-ph/2021/05/31/microsoft-launches-first-asia-pacific-public-sector-cyber-security-executive-council-across-seven-markets-in-the-region/.

101 Association of Southeast Asian Nations and Electronic Transactions Development Agency, 'ASEAN Critical Information Infrastructure Protection Framework', 2020. This study involved input from member states' coordinating authorities and national cyber-security experts.

102 Ralf Emmers, 'ASEAN Minus X: Should This Formula Be Extended?', RSIS Commentary, CO17199, 24 October 2017, https://www.rsis.edu.sg/rsis-publication/cms/co17199-asean-minus-x-should-this-formula-be-extended/#.YXwPt_pByF4.

103 The 'ASEAN minus X' model was used in the 2007 ASEAN Convention on Counter-Terrorism and the 2015 ASEAN Convention Against Trafficking in Persons, Especially Women and Children. See Yoshifumi Fukunaga, 'Use of Legal Instruments in the Economic Community Building', *Journal of Contemporary East Asia Studies*, vol. 10, no. 1, April 2021, pp. 78–79.

104 For an example of a cyber lexicon, see that compiled by the Financial Stability Board, an international body that monitors the global financial system: Financial Stability Board, 'Cyber Lexicon', 12 November 2018, https://www.fsb.org/2018/11/cyber-lexicon/.

105 Under the ARF ISM on ICTs Security, points-of-contact directories have been created to facilitate operational coordination during routine incidents and incidents of regional significance. The directories can include either a single coordination point of contact within the government or multiple contacts from diplomatic, national-security and policy coordination, law enforcement, or technical agencies. See ASEAN Regional Forum, 'Concept Paper by Australia-Malaysia: ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs)', March 2019, https://aseanregionalforum.asean.org/wp-content/uploads/2019/06/ANNEX-4-Comments-on-CBM1-Final-Concept-Paper-24-May-Clean.pdf.

106 ASEAN signed a Treaty on Mutual Assistance in Criminal Matters in 2004 to enhance mutual legal assistance in criminal matters, but its scope to address cyber threats is limited. See Vision of Humanity, 'ASEAN Must Enhance Cross-border Alignment on Cybercrime Laws', n.d., https://www.visionofhumanity.org/asean-needs-to-enhance-cross-border-cooperation-on-cybercrime/.

107 ASEAN Coordinating Centre for Humanitarian Assistance on Disaster Management, 'ASEAN-ERAT – ASEAN Emergency Response and Assessment Team', November 2017, p. 6, https://ahacentre.org/files/ASEAN-ERAT-FAQ.pdf. ASEAN-ERAT teams are formed by drawing members from the National Disaster Management Office (NDMO) and other relevant government authorities, including the private sector, international bodies and academia.

108 Andrea Calderaro and Anthony J. S. Craig, 'Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building', *Third World Quarterly*, vol. 41, no. 6, June 2020, pp. 917–938, https://doi.org/10.1080/01436597.2020.1729729.

109 United Nations General Assembly, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', A/76/135, 14 July 2021, p. 14, https://namib.online/wp-content/uploads/2021/08/2021-07-14_eng_A_76_135-2104030E-1.pdf.

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington, DC 20037 | USA
t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GBCORP Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org