DIGITAL DIALOGUE

Cyber Diplomacy in Southeast Asia

Nathalie Van Raemdonck,
Vrije Universiteit Brussels

May 2021

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.

Contents

Executive summary

South-East Asian countries are taking huge strides in improving the region's cybersecurity through the Association of Southeast Asian Nations (ASEAN), creating collective resilience and protecting critical infrastructures, while being conscious the differences in countries' maturity and capacity. The region is an important partner for the European Union (EU) in creating global stability in cyberspace, as it balances several geopolitical perspectives on what stability means. Voting behaviour of South-East Asian states in international fora has reflected this balancing exercise, brokering between proposals that reflect a state-centric view on cyber security governance and a market-based multi-stakeholder view on cyberspace, which they do not see as necessarily contradictory.

Key takeaways:

- ASEAN member states created a Ministerial Conference on Cybersecurity (AMCC), which developed a regional strategy on cybersecurity and resilience protection. A coordinating committee on cybersecurity (ASEAN Cyber-CC) is mandated to work cross-sectorally with relevant representatives from sectoral bodies on cybersecurity issues.
- The region lacks a general overarching regulation on cybercrime, even though there is serious cooperation on cybercrime between ASEAN member states, with a dense network of bilateral mutual legal assistance treaties. Discussions in the ASEAN Regional Forum show that as yet there is no common understanding on the definition of cybercrime, nor a common approach to address this issue. Many ASEAN states' policy on cybercrime is focused more on avoiding social disruptions and controlling the spread of disinformation than on technology issues.
- Conversations on confidence-building in the ASEAN Regional Forum have fostered renewed cooperation between major global actors that have a stake in South-East Asia. The conversation on confidence-building measures (CBMs) shows a promising avenue to exchange perspectives. There is, however, a lack of trust in the information-sharing infrastructure, and there are some major differences in national perceptions regarding cyberspace threats and challenges.
- Digital single market aspirations encounter some barriers, such as the digital divide of the region and data protection regulations of some countries that require data about their citizens to be stored on local servers. There is knowledge exchange with the EU on the creation of digital single markets.
- ASEAN member states have subscribed in principle to the 11 voluntary, non-binding norms set out in the 2015 report by the UN Group of Governmental Experts (UNGGE) instead of developing new norms, and are cooperating towards practical implementation of the UNGGE norms. How exactly ASEAN member states will observe the norms they have adopted when actual incidents occur is as yet unclear. ASEAN states have so far refrained from 'naming and shaming' as they lack the means to accurately attribute the true source of cyberattacks. Apart from a general statement that international law is applicable in cyberspace, the region lacks a perception of the application of international law.
- ASEAN tries not to choose between exclusive state-centric cybersecurity governance and an unsupervised, market-based multi-stakeholder approach, but elects to be a 'broker' between the Chinese and American styles of cybersecurity governance. The 2018 Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) is an important tool of digital autonomy in the US–China trade war. It reduces the dependency of ASEAN members on both Chinese and US trading and manufacturing, while strengthening ties with Latin America.

- The EU regards support of ASEAN's inclusive multilateral architecture in the region as an important objective, as it sees ASEAN as a peaceful influencer in the region. The EU has crystallised cybersecurity as a priority in its cooperation with all Asian countries. In a 2019 joint statement on cybersecurity cooperation, the EU and ASEAN committed to contribute to the advancement of an open, secure, stable, accessible and peaceful information and communications technology (ICT) environment. While this is a notable effort, the EU is challenged by cultural differences when it comes to the exact interpretations of these terms. The EU's policy initiatives mostly focus on supporting capacity-building efforts in states that are at a low maturity level, and on working and increasing cooperation in multilateral fora.

1 General Regional Profile: What typifies South-East Asia in cyberspace?

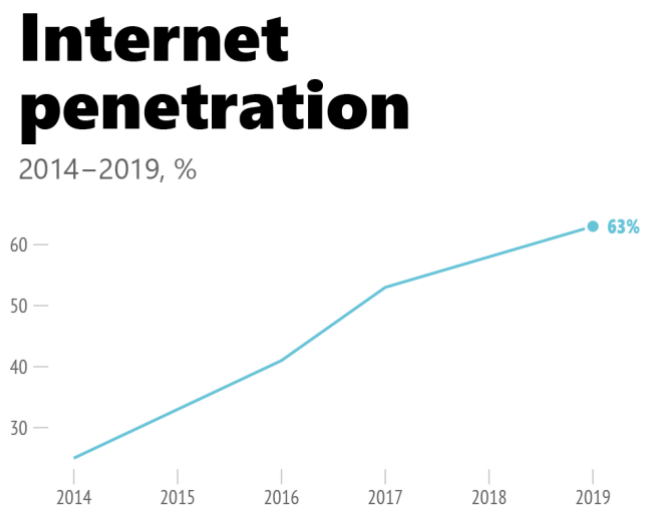
For the European Union (EU), engagement with Asian-Pacific countries is essential to build a secure and rights-based global cyberspace. However, the region is immensely diverse and requires several different collaboration structures. It therefore does not lend itself to generalisations or overviews that assume a certain coherence.

On digital transformation alone, the region is full of discrepancies. It includes pioneering countries such as Japan, Singapore and South Korea that are leading the digital revolution in Asia and the world, but also developing countries such as Cambodia, Laos and Myanmar, which until five years ago barely had any internet access. The two countries with the world's biggest population, China and India, also contribute to this discrepancy. While these giants are undergoing a massive digital transformation, the degree of digitalisation and digital practices varies within their national territories.

To retain focus, this paper will limit itself to the group of South-East Asian states that are connected through the Association of Southeast Asian Nations (ASEAN) and its interactions with partners in the region.[1] It will investigate the engagement cooperation ASEAN has had with the European Union, and where the potential lies for congruency to increase stability in cyberspace.

1.1 Connectivity

About 63% of the population in South-East Asia were connected to the internet in 2019.[2] This number has been rising quickly, with an estimated 125,000 new users gaining internet access daily since 2014.[3] Six years ago, internet penetration had not risen above 25% for the region, but the mobile boom changed this significantly. Mobile devices have become the main entry point for internet access for most people in the region.[4]



Data: International Telecommunication Union (ITU) via the We Are Social Global Digital Reports

[1] For a focus on Japan, Korea, India and China, see the dedicated dialogue papers at www.eucyberdirect.eu
[2] Internet World Stats, last accessed 9 March 2020. https://www.internetworldstats.com/stats3.htm#asia
[3] World Economic Forum: Digital ASEAN initiative, last accessed 19 January 2021. https://www.weforum.org/projects/digital-asean
[4] PwC Growth Markets Centre (2018) 'The Future of ASEAN – Time to Act'. https://www.pwc.com/sg/en/publications/assets/healthcare-future-asean-2018.pdf

1.2 Vulnerabilities

The region's cyberspace in general has been highly targeted by cyber-operations. A few facts on threat actors and vulnerabilities paint an interesting picture:

- A study by FireEye in 2016 showed that Asia-Pacific in general was **80% more likely to be targeted** by hackers than the rest of the world.[5] Specifically for South-East Asia, the Philippines ranked fourth in the world in terms of where online threats were detected, followed by Malaysia at 13th and Vietnam at 17th.[6]
- Cybersecurity company Kaspersky detected 14 million phishing attempts for user credentials in South-East Asia in the first half of 2019.[7] In the same period, Singapore and Malaysia recorded the **highest business email attacks** in the region, respectively 54% and 20% of the total attacks in the region.[8]
- According to another 2016 study, **cybercrime** inflicted **$81 billion** in damage in all of Asia-Pacific.[9]
- Since mobile is a main entry point for citizens to go online, it is also a significant attack vector in South-East Asia. Indonesia stood 6th and Malaysia 10th globally as countries most affected by **mobile malware**.[10]
- South-East Asian countries often serve as **launchpads or hub for attacks** worldwide. This is due to vulnerable infrastructure which can be exploited and to the region's well-connectedness to global connections.[11]

The cybersecurity industry assessed most countries in the region to be severely lacking in resilience.[12] The more prosperous countries have difficulty in securing their wide attack surface, which is increasingly expanding with Internet of Things (IoT) devices, smart cities and Big Data applications. Singapore, which has been pioneering this trend with its Smart Nation initiative, became very aware of its vulnerability after the data breach at Singapore Health Services (Singhealth) in 2018. Over 1.5 million patients' data was exfiltrated during this breach, including that of Singapore's prime minister.[13]

1.3 Threat Actors

One of the main threat actors for the region is China, which uses cyberattacks strategically over South China Sea issues. Maritime South-East Asia has experienced several incidents of cyber-espionage, and the Permanent Court of Arbitration Tribunal on the South China Sea dispute ruling has seen activities by Chinese Advanced Persistent Threat (APT) groups.[14] There have also been espionage operations

[5] FireEye (2018) 'Cyber Evolution: En Route to Strengthening Resilience in Asia-Pacific'. https://www.fireeye.com/offers/wp-cyber-evolution-apac.html

[6] INTERPOL (2020) 'ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk'. https://www.interpol.int/en/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf

[7] ibid.

[8] ibid.

[9] Marsh & McLennan Companies (2017) 'Cyber Risk in Asia-Pacific: The Case for Greater Transparency'. Asia Pacific Risk Center.

[10] Kaspersky (2019) 'Mobile Malware Evolution 2019'. https://securelist.com/mobile-malware-evolution-2019/96280/

[11] Kearney (2018) 'Cybersecurity in ASEAN: An Urgent Call to Action'. https://www.southeast-asia.kearney.com/web/southeast-asia/article?/a/cybersecurity-in-asean-an-urgent-call-to-action

[12] ibid.

[13] Kwang, Kevin (2018) 'Singapore Health System Hit By "Most Serious Breach Of Personal Data" In Cyberattack; PM Lee's Data Targeted'. Channelnews Asia. https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318

[14] Said, Farlina (2019) 'Major Powers Cyber Competition in the Region', in Christian Fitriani Pareira & Naufal Armia Arifin, Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia, Centre for Strategic and International Studies.

surrounding the Malaysia MH370 investigations, a 2016 hack on Vietnamese airports[15] and the compromising of Vietnamese intelligence networks after an incident over a Chinese oil rig in Vietnamese-claimed waters in 2014.[16] Chinese-linked threat actors launched phishing attacks with COVID-19 disinformation on Vietnamese targets during the global pandemic in 2020.[17]

As well as abusing cyberspace for geopolitical purposes, China has a high demand for confidential information, which manifests in the form of espionage and IP theft.

As well as abusing cyberspace for geopolitical purposes, China has a high demand for confidential information, which manifests in the form of espionage and IP theft. This is driven by the need to develop technologies that would reduce reliance on technologies that are out of Chinese control.[18] These operations are particularly targeting private sector organisations.[19] The Australian Strategic Policy Institute (ASPI) saw a reduction of such espionage around 2017, presumably because the country increased its development of indigenous intellectual property.[20]

North Korea is also a threat actor for the region. Since 2011, the Lazarus Group, which is suspected to run under the command of the North Korean regime, has been targeting banks in South Korea, the Philippines and Vietnam, the Bangladesh bank cyber heist in 2016 being the most notorious attack in Asia. North Korea greatly expanded its cyber activities for monetary gains globally and regionally. It has also been responsible for numerous attacks on cryptocurrency exchanges in South-East Asia.[21] The Wannacry ransomware campaign that wreaked havoc all over the world affected hospitals in Indonesia.[22]

[15] Ibid.

[16] Piiparinen, A. (2016) China's Secret Weapon in the South China Sea: Cyber Attacks. The Diplomat, 22 July. https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/

[17] Insikt Group (2020) 'Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide'. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pDf

[18] Xinhua (2016) 'President Xi Says China Faces Major Science, Technology "Bottleneck"'. Xinhua News Agency, 1 June. http://www.xinhuanet.com/english/2016-06/01/c_135402671.html

[19] FireEye (2018) 'Cyber Evolution: En Route to Strengthening Resilience in Asia-Pacific'. https://www.fireeye.com/offers/wp-cyber-evolution-apac.html

[20] Australian Strategic Policy Institute (2017) 'Cyber Maturity: ASPI 2017 Report'.
For more info on China's cybersecurity strategy, see EU Cyber Direct's dedicated paper on China's Cyber diplomacy.

[21] Haynes, Matthew (2018) 'State Sponsored Actors Focus Attacks on Asia'. Bleeping Computer. https://www.bleepingcomputer.com/news/security/state-sponsored-actors-focus-attacks-on-asia/

[22] Said, Farlina (2019) 'Major Powers Cyber Competition in the Region', in Christian Fitriani Pareira & Naufal Armia Arifin, Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia. Centre for Strategic and International Studies.

2 Institutional Landscape

Historically caught between superpowers China, Russia and the US, the countries in Asia Pacific, and specifically South-East Asia, know how to navigate their national interests while balancing security. South-East Asia has been an arena for great powers to extend their influence in global politics, specifically during the Cold War. During that time, alignment towards the US or the Soviet Union divided the region.[23]

The struggle for autonomy is one of the reasons why ten South-East Asian countries created ASEAN.[24] The cooperation organisation allowed states to increase their bargaining power and demand respect for their sovereignty. It also fostered inclusive cooperation, creating an 'ASEAN way'. This ASEAN way prioritises consultation and consensus in decision-making, along with respect for sovereignty and non-interference in internal affairs.[25] Built around the ASEAN architecture are several cooperation mechanisms such as the ASEAN Regional Forum, the East Asia Summit and Asia-Pacific Economic Cooperation.

2.1 Regional Architecture

ASEAN

The ASEAN secretariat does not provide coordinators to follow up and implement agreements: it only provides administrative support. Usually member states take the lead in assisting other countries and exchanging best practices.

Cybersecurity has been discussed in several sectoral ministerial bodies: the ASEAN Foreign Ministers' Meeting (AMM), the ASEAN Defense Ministers' Meeting (ADMM), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) and the Telecommunications and Information Technology Ministers' Meeting (TELMIN), which in 2019 became the ASEAN Digital Ministers Meeting (ADGMIN).[26] To streamline the discussion, ASEAN member states started the informal Ministerial Conference on Cybersecurity (AMCC) in 2016.[27] This group identified an ASEAN cybersecurity strategy in 2018.[28]

In 2018 the Telecommunications and Information Technology Senior Officials' Meeting (TELSOM) (which in 2019 became the ASEAN Digital Senior Officials' Meeting (ADGSOM)) decided that the ASEAN Network Security Action Council (ANSAC) would prepare a proposal for a formal ASEAN cybersecurity coordination mechanism.[29] This resulted in the establishment of the ASEAN Coordinating Committee on Cybersecurity (ASEAN-Cyber CC), which was inaugurated at the end of 2020.[30] The terms of reference were drafted by the ANSAC. This coordination committee will complement existing efforts on capacity building in ASEAN by the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC).

ASEAN Regional Forum

Several forums are based on the structure of the core group of ten ASEAN states. The ASEAN Regional Forum (ARF), established in 1994, is the most important organisation in terms of security and regional

[23] Weatherbee, Donald (2014) International Relations in Southeast Asia: The Struggle for Autonomy. Rowman & Littlefield.
[24] Member states are Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam.
[25] Jones, Lee (2010) 'ASEAN's Unchanged Melody? The Theory and Practice of "Non-interference" in Southeast Asia'. Pacific Review, 23, no. 4.
[26] Association of Southeast Asian Nations (ASEAN) (2019) 'Chairman Statement'. 35th ASEAN Summit.
[27] Cyber Security Agency Singapore (2016) 'ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN'. https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean#sthash.N2wSyXLM.h5MpHQiy.dpuf
[28] Association of Southeast Asian Nations (ASEAN) (2018) 'Leaders' Statement on Cybersecurity Cooperation Strategy'. 32nd ASEAN Summit.
[29] Association of Southeast Asian Nations (ASEAN) (2018) 'Chairman Statement'. 33rd ASEAN Summit.
[30] Association of Southeast Asian Nations (ASEAN) (2020) 'Chairman Statement'. 37th ASEAN Summit.

stability.[31] The ARF, which is institutionally part of the ASEAN Community Council, has a very diverse composition. Apart from the ten ASEAN member states and most other Asian countries, it also includes Russia and China, as well as Western allies the EU, Canada, Australia and the United States. The key guiding principles of the forum are preventative diplomacy and confidence-building. Although progress is slow and incremental, the ARF offers a relevant platform to promote a stable and secure cyberspace.

The key guiding principles of the forum are preventative diplomacy and confidence-building. Although progress is slow and incremental, the ARF offers a relevant platform to promote a stable and secure cyberspace.

The ARF developed a work plan in 2015 on information and communications technologies security. Its objectives were to develop confidence-building measures to avoid misperceptions, improve cooperation to respond to criminal and terrorist use of ICT, and cooperate to develop resilient government ICT environments. [32] It specified some practical measures: sharing of information on laws, policies and practices; holding exercises to prevent incidents from becoming regional security problems; exchanging lessons learned from dealing with threats.

Since its establishment in 2017, there has been gradual progress on the implementation of this work plan through the ARF's Inter-Sessional Meetings (ISMs) on ICT security. An Open-Ended Study Group (OESG) was created to discuss CBMs that can reduce the risk of conflict stemming from the use of ICT. The OESG is an expert-level body subordinated to the ISM, allowing for in-depth debates with a view to building consensus. There have been five OESGs since 2018, of which the ISM adopted three proposals in total.

East Asia Summit

The East Asia Summit (EAS), established in 2005, was based on the ASEAN plus 6 mechanism, (now ASEAN plus 8). It comprises 18 members, and annually brings together ASEAN members, other major Asia-Pacific players, Russia and the United States.[33] The EU's request for membership is currently pending. The focus of this summit is more economic, with a community-building aspect.

In 2015 the leaders of the EAS adopted a statement on issues related to security of and in the use of ICT, where they decided that EAS countries should endeavour to strengthen national and regional stability in this field.[34] No concrete actions seem to have been taken on this statement, but the commitment was reaffirmed in the 2017 Chairman's statement[35] and expanded on in the 2018 Leaders' Statement on Deepening Cooperation in the Security of ICTs and the Digital Economy.[36] While the EAS has no operational capacities, it provides a fruitful forum for countries in the region to engage in discussion and explore bilateral and bi-regional cooperation, such as in the recent ASEAN–Japan Capacity Building Centre or the Singapore–Australia 2020 workshop on regional cyber capacity building.

[31] Members: ASEAN (Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam), Australia, Bangladesh, Sri Lanka, Canada, China, Democratic People's Republic of Korea, European Union, India, Japan, Mongolia, New Zealand, Pakistan, Papua New Guinea, Republic of Korea, Russia, Timor-Leste, United States.

[32] ASEAN Regional Forum (ARF) (2015) 'Workplan on Security of and in the Use of Information and Communications Technologies (ICTs)'.

[33] Members: ASEAN (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam), Australia, China, India, Japan, New Zealand, the Republic of Korea, the United States and Russia.

[34] East Asia Summit (EAS) (2015) 'Statement on Issues Related to Security of and in the Use of Information and Communications Technologies', Kuala Lumpur, Malaysia. 10th East Asia Summit.

[35] East Asia Summit (EAS) (2017) Final Chairman's Statement of the 12th East Asia Summit', Pasay, the Philippines.

[36] East Asia Summit (EAS) (2018) 'Leaders' Statement on Deepening Cooperation in the Security of Information and Communications Technologies and of the Digital Economy'. Singapore, 13th East Asia Summit.

APEC

Asia-Pacific Economic Cooperation (APEC), established in 1989, is a forum of 21 Asia-Pacific, North American and South American countries and Russia, all bordering the Pacific Ocean.[37] Its primary focus is to improve trade relations. Some of the APEC countries are also part of the CPTPP, a free-trade deal connecting the Pacific region. This agreement is relevant to the digital economy as it has a clause on e-commerce.

APEC hopes to build an Asia-Pacific Information Society (APIS) and is supported in this endeavour by the Telecommunications and Information Working Group (TEL WG), which began its work in 1990. The TEL WG included cybersecurity in its Strategic Action Plan for 2016–2020 to build a secure, resilient and trusted ICT environment.[38] TEL WG conducts the cybersecurity part of its work programme in the Security and Prosperity Steering Group (SPSG).[39] The SPSG initially aimed to create a cybersecurity framework, led by Thailand, but changed course to create an APEC Framework for Securing the Digital Economy. This unfortunately narrowed the focus from the more comprehensive framework on cybersecurity initially intended.[40] The five-year strategic action plan 2021–2025 is still being drafted at the time of publication.

[37] Members: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, the Russian Federation, Singapore, Chinese Taipei, Thailand, United States of America, Vietnam.

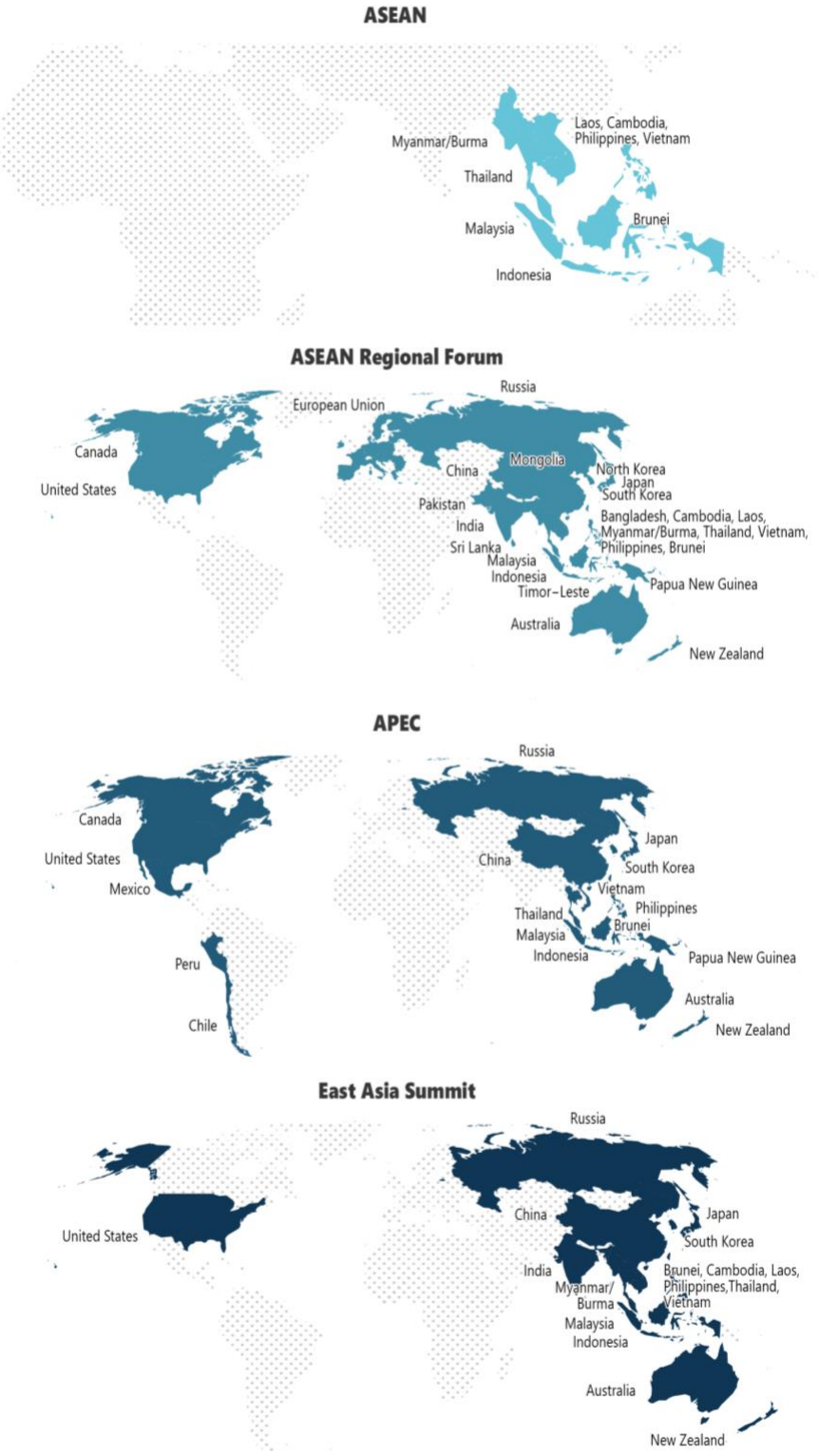
[38] Asia-Pacific Economic Cooperation (APEC) (2015) 'Telecommunications and Information Working Group Strategic Action Plan 2016–2020'.

[39] Asia-Pacific Economic Cooperation (APEC) 'Telecommunications and Information Working Group', last accessed 18 March 2019. https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

[40] Asia-Pacific Economic Cooperation (APEC) 'Telecommunications and Information Working Group', last accessed 18 March 2019. https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

Regional cooperation

Membership



Data: European Comission 2021

Institutions	Description
ASEAN	**Association of Southeast Asian Nations**
ASEAN-Cyber CC	The ASEAN Coordinating Committee on Cybersecurity comprises representatives from relevant sectoral bodies to strengthen the cross-sectoral coordination on cybersecurity within ASEAN.
AMCC	The ASEAN Ministerial Conference on Cybersecurity discusses cyber resilience and norms in cyberspace.
ANSAC	ASEAN Network Security Action Council predates the AMCC and is jointly responsible for formalising a framework for cybersecurity engagement in ASEAN.
TELMIN → ADGMIN TELSOM → ADGSOM	The Telecommunications and Information Technology Ministers Meeting (TELMIN) was responsible for digital affairs and digital economy, and reformed to the ASEAN Digital Ministers Meeting (ADGMIN). It also hosted the TELSOM, the Senior Official's Meeting – now the ASEAN Digital Senior Officials Meeting (ADGSOM).
ADMM	The ASEAN Defence Ministers' Meeting created an Expert Working Group on Cyber Security.
AMMTC	The ASEAN Ministerial Meeting on Transnational Crime hosts the Senior Officials' Meeting on Transnational Crime (SOMTC), which has set up the ASEAN working group on cybercrime.
ASCCE	The ASEAN–Singapore Cybersecurity Centre of Excellence will be responsible for executing part of the cybersecurity strategy, and will function as a think-tank and training centre.
AJCCBC	The ASEAN–Japan cybersecurity capacity building centre will train cybersecurity workforces in governmental agencies and critical infrastructures.
ARF	**ASEAN Regional Forum**
ARF ISM on ICT Security	The ARF's Inter-Sessional Meetings (ISMs) on ICT Security convene yearly to discuss CBMs.
OESG	The Open Ended Study Group (OESG) on Confidence Building Measures is an expert-level body subordinated to the ISM, which allows in-depth debates with a view to building consensus.
EEPG	The Experts and Eminent Persons Group is a group of state and non-state actors that provide reports and support to the ARF meetings.
APEC	**Asia-Pacific Economic Cooperation**
TEL WG	The Telecommunications and Information Working Group supports developments of ICT policies in the Asia-Pacific region.
SPSG	The Security and Prosperity Steering Group is part of the TEL WG; it organises incident management exercises and best-practices workshops across the Pacific region.

2.2 Non-governmental actors

ASEAN states generally favour national authority over a multi-stakeholder approach. Some private sector organisations hold the perception that states see citizens as entities that must be managed rather than partnered with.[41] Some governments in ASEAN are cautious about sharing information with the

[41] Marsh & McLennan Companies (2017) 'Cyber Risk in Asia-Pacific: The Case for Greater Transparency'. Asia Pacific Risk Center.

private sector, the technical community and citizens (e.g. ethical hackers). There is, however, a gradual acceptance of the private sector and other stakeholders' involvement in the region.

This turn towards openness was demonstrated in the ASEAN 2018 cybersecurity cooperation strategy, where members recognised the value of enhanced dialogue and cooperation on cybersecurity issues with other external parties.[42] The newly created ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) prides itself on being an open and inclusive platform, where all stakeholders from industry, academia and international organisations are welcome to participate.[43]

A few initiatives put this inclusion into practice. The 2018 ASEAN Ministerial Conference on Cybersecurity made an industry call for innovation in collaboration with five participating organisations: the Ascendas-Singbridge Group, PacificLight Power, Singapore LNG Corporation, SMRT Corporation and Singapore Press Holdings.[44] Singapore's Monetary Authority (MAS) also established the Asia-Pacific Regional Intelligence and Analysis Centre in 2016 together with the financial sector's FS-ISAC. [45] This real-time information sharing platform of cyber-threat indicators was later joined by the Singapore Cybersecurity Agency (CSA), the first of its kind in terms of cooperation with the private sector.[46] ASEAN member states are taking this one step further by establishing the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) to share threat intelligence and best practices among members of the Digital Technology Network (DTN).[47]

Singapore also launched a government bug bounty programme in 2018, where, for a reward, selected white-hat hackers were invited to test specific defence systems for vulnerabilities.[48] The ARF has regularly involved the technical community by inviting experts from the Asia-Pacific Network Information Center (APNIC). It has also involved the national computer security incident response teams (CSIRTs) to operationalise cyber CBMs, and it regularly allows a group of 'expert and eminent persons' to provide reports to its meetings.[49]

The global discussion on responsible behaviour in cyberspace is increasingly involving more than just governments in South-East Asia. Think-tanks and academia are already regularly involved in the regional policy-making process through Track Two diplomacy initiatives. A dozen strategic study centres formed the Council for Security Cooperation in the Asia-Pacific (CSCAP) in 1993. A study group at CSCAP proposes cyber norms and CBMs to the ARF's ongoing ISM on ICT security in 2018.[50] Think tanks in the region also launched a Track 1.5 initiative led by the Australian Strategic Policy Institute (ASPI). The Sydney initiative proposed practical futures for cyber norms and confidence building.[51] Despite good intentions and proactive initiatives from experts, ASEAN is not involving stakeholders in international

[42] Association of Southeast Asian Nations (ASEAN) (2018) 'Leaders' Statement on Cybersecurity Cooperation Strategy'. 32nd ASEAN Summit.

[43] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[44] Cyber Security Agency of Singapore (2018) 'Singapore International Cyber Week 2018: Highlights and Testimonials'. https://www.csa.gov.sg/news/press-releases/sicw-2018---highlights-and-testimonials

[45] Monetary Authority of Singapore (2016) 'FS-ISAC and MAS Establish Asia Pacific (APAC) Intelligence Centre for Sharing and Analysing Cyber Threat Information'. http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx

[46] Cybersecurity Agency of Singapore (2018) 'FS-ISAC and CSA Partner to Enhance Cybersecurity in Singapore'. https://www.csa.gov.sg/news/press-releases/fs-isac-and-csa-partner-to-enhance-cybersecurity-in-singapore

[47] Association of Southeast Asian Nations (ASEAN) (2020) 'Chairman Statement'. 37th ASEAN Summit.

[48] Lim, Min Zhang (2018). 'Hackers Find 35 Bugs in First Mindef Bug Bounty Programme, $19,500 Paid Out.' Straits Times. www.straitstimes.com/singapore/hackers-find-35bugs-in-first-mindef-bug-bounty-programme-19500-paid-out

[49] ASEAN Regional Forum (ARF) (2015) 'Summary Report ARF Seminar on Operationalizing Cyber Confidence Building Measures'.

[50] Council for Security Cooperation in the Asia-Pacific (CSCAP) (2018) 'Developing Cyber Norms of Behaviour and Confidence Building Measures for Asia Pacific'.

[51] Australian Strategic Policy Institute (ASPI) (2018) 'Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN Region'. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-09/Sydney%20recommendations_Cyber-ASEAN.pdf?kwrNP4FHCYxE9oGVhxzchUvF3rx11oG

discussions as much as other regions in the world. The closed regional consultation of the UNGGE chair with ASEAN in 2019 was an unfortunate demonstration where non-state actors were not allowed to participate in creating a common position for the region. There was some multi-stakeholder exchange of views at the 2019 Singapore Cyber Week where the regional consultation took place, but this was restricted to the panelists of the 'invitation only' leaders' symposium.[52]

> **Despite good intentions and proactive initiatives from experts, ASEAN is not involving stakeholders in international discussions as much as other regions in the world.**

The community of digital rights activists is even less engaged in the region. Existing organisations primarily focus on press freedom, and seem less developed and outspoken on cybersecurity issues. Lack of openness from state actors can be a reason why these digital rights organisations are not very developed, as there is little margin for engagement. The technical community is more involved in the region: for example, APNIC, the regional IP registry organisation, and the collaboration of cyber emergency response teams (CERTs), which have gathered in the Asia-Pacific Computer Emergency Response Team (APCERT) since 2003.

In Thailand, an initiative that is the first of its kind seems to pioneer multi-stakeholder engagement on cybersecurity. Manushya, a civil society organisation created in 2017, organised experts' meetings with government and political representatives and created a recommendation report for the Thai authorities to build a human-centred cybersecurity act.[53] The initiative's aim is to help build the discourse on the necessity of applying a human rights-based approach to cybersecurity legislation.[54] If successful, this model could be adapted by the developing civil society community in the region.

Stakeholders	Description
Private sector	
Asia-Pacific Regional Intelligence and Analysis Centre	This real-time information-sharing platform of cyber-threat indicators was established by the Singapore's Monetary Authority (MAS) together with the Financial Services Information Sharing and Analysis Center (FS-ISAC).
CRISP	The ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) was established as a platform for sharing of threat intelligence and best practices between members of the Digital Technology Network (DTN)
Think-tanks	

[52] United Nations Office of Disarmament Affairs (2019) 'Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf

[53] Manushya Foundation (2019) 'Thailand's Cybersecurity Act: Towards a Human Centered Act Protecting Online Freedom and Privacy, While Tackling Cyber Threats'. https://www.manushyafoundation.org/study-on-cybersecurity-act

[54] Access Now (2019) 'In Thailand, a Promising New Initiative for Human-Centered Cybersecurity'. https://www.accessnow.org/in-thailand-a-promising-new-initiative-for-human-centered-cybersecurity/

CSCAP	The Council for Security Cooperation in the Asia-Pacific has a study group on cybernorms that advises the ARF.
ASEAN-ISIS	ASEAN Institutes of Strategic and International Studies
National think-tanks	• Centre for Strategic and International Studies (CSIS), Indonesia • Institute for Strategic and International Studies Malaysia (ISIS Malaysia), • Institute of Security and International Studies Thailand (ISIS Thailand) • Myanmar Institute of Strategic and International Studies (MISIS) • Stratbase ADR Institute for Strategic and International Studies (ADRi), Philippines • S. Rajaratnam School of International Studies (RSIS), Singapore • Singapore Institute of International Affairs (SIIA) • ISEAS-Yusof Ishak Institute (Singapore) • Diplomatic Academy, Vietnam • Institute of Foreign Affairs (IFA) Lao People's Democratic Republic • Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (BDIPSS), Brunei Darussalam • Institute for Cooperation and Peace (CICP), Cambodia

Technical community

APNIC	The Asia-Pacific Network Information Center is the regional IP registry organisation.
ISOC	The Internet Society is an international organisation that provides advice to protect the internet infrastructure.
APT	The Asia-Pacific Telecommunity is a joint initiative of the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) and the International Telecommunication Union (ITU), and contributes to development and growth of the ICT sector in the region.
APCERT	The Asia-Pacific Cyber Emergency Response Team is a forum created in 2003 for the community of all CERTs in the region, focusing on technical coordination.

3 Policy issues, priorities and actions

To tackle the threats that come with digital transformation, the ten member states of ASEAN and its partner countries have been engaged in improving cybersecurity through regional cooperation. A major digital divide between South-East Asian countries has, however, raised the question: is there a need for cybersecurity if there is no cyber space?[55] A different digital space creates a different threats landscape. Cybersecurity has therefore developed at different speeds in the region, where cooperation has been based on consensus with respect for regional sovereignty.

A dilemma of priorities plagues all South-East Asian countries: are state actors and cybercriminals the biggest threat stemming from cyberspace, or are domestic issues playing out over the internet in the form of disinformation and terrorism a bigger threat?

A dilemma of priorities, however, plagues all South-East Asian countries: are state actors and cybercriminals the biggest threat stemming from cyberspace, or are domestic issues playing out over the internet in the form of disinformation and terrorism a bigger threat?[56] The concern over information operations in ASEAN is genuine. Campaigns of disinformation have been blamed for social unrest and violence in Indonesia and the Philippines.[57] Governments and political parties themselves are not reluctant to use disinformation operations against their own population.[58] Cyber conversations on domestic concerns are, however, shied away from in regional conversations, and they have only recently become a topic in ASEAN regional dialogues due to the COVID-19 pandemic and health-related misinformation. The regional engagement strategies so far focused on external cybersecurity threat actors. ASEAN states have been creating effective cybersecurity cooperation in the past few years on this priority that all states could agree on.

3.1 Resilience

As of early 2021, Singapore, Malaysia, Thailand the Philippines have laid out a national cybersecurity strategy. Singapore, Malaysia and the Philippines each have a dedicated national agency to implement the national cybersecurity strategy. In other ASEAN countries, responsibilities are scattered across government institutions. The national CERTs often play the role of national cybersecurity agencies. This role is only reactive, and they often do not have the mandate to work preventatively or improve national and regional cooperation. For the countries that do not have much digital infrastructure to secure, there seems to be no real urgency for cybersecurity. [59] This is why collective resilience was pushed onto the ASEAN agenda in recent years. Efforts to streamline the discussion led to the informal Ministerial Conference on Cybersecurity (AMCC) in 2016. This yearly meeting, which built on the Meeting of the ASEAN Telecommunications and IT Ministers (TELMIN), was meant to identify an appropriate ASEAN

[55] Krisetya, Beltsazar (2019) 'Examining Southeast Asia's Cyber Terrain', in Christian Fitriani Pareira & Naufal Armia Arifin, *Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia*, Centre for Strategic and International Studies.

[56] Christian Fitriani Pareira & Naufal Armia Arifin, *Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia*, Centre for Strategic and International Studies.

[57] Ang, Benjamin (2020) 'Singapore, ASEAN and international cybersecurity', in Eneken Tikk & Mika Kerttunen, *Routledge Handbook of International Cybersecurity*, Routledge.

[58] Kajimoto, Masato (2018) 'In East and Southeast Asia, Misinformation Is a Visible and Growing Concern'. Poynter. https://www.poynter.org/fact-checking/2018/in-east-and-southeast-asia-misinformation-is-a-visible-and-growing-concern/

[59] Krisetya, Beltsazar 'Examining Southeast Asia's Cyber Terrain', in Christian Fitriani Pareira & Naufal Armia Arifin, Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia, Centre for Strategic and International Studies.

platform for discussing regional cybersecurity strategy and cooperation.[60] From these gatherings, a 2018 ASEAN cybersecurity strategy was found for the region. Up until that point, there was not even a common definition and scope of cybersecurity between ASEAN member states.[61]

> **The ASEAN Cybersecurity Strategy calls for greater regional cooperation in cybersecurity policy development, diplomacy and capacity building in several sectoral fora, which helped establish the ASEAN Coordinating Committee on Cybersecurity (ASEAN Cyber-CC) in late 2020.**

This strategy called for greater regional cooperation in cybersecurity policy development, diplomacy and capacity building in several sectoral fora.[62] Singapore was mandated to draft the ASEAN Cybersecurity Coordination Mechanism Paper in 2019, which culminated in the ASEAN Coordinating Committee on Cybersecurity (ASEAN Cyber-CC) in late 2020. This Coordinating Committee will work cross-sectorally with relevant representatives from sectoral bodies on cybersecurity issues.[63]

The AMCC was also tasked to develop a set of practical cybersecurity norms of behaviour in ASEAN. It agreed on this in 2018 at the third AMCC, by subscribing in principle to the 11 voluntary non-binding norms of responsible behaviour for states that had been identified by the UNGGE in 2015.[64] At the 2019 AMCC, it agreed to establish a working-level committee to implement these norms, an effort that is chaired by Malaysia.[65] During several ASEAN capacity-building workshops, cyber experts of member states identified areas where progress has been made, as well as other areas in need of capacity building in order to successfully implement the norms. The working-level committee based itself on these experiences to study and propose recommendations.[66] Malaysia shared the progress of the ASEAN plan of action on the implementation of norms of responsible states' behaviour in cyberspace with ASEAN member state and dialogue partners at the 5th AMCC in 2020.[67]

To build operational, policy and legal capacity in all ASEAN member states, the ASEAN Cyber Capacity Programme was created in 2017, primarily funded by Singapore. As an extension to this programme, Singapore also established the ASCCE in 2019, which executes parts of the regional cybersecurity strategy. The ASCCE functions as a cyber think-tank and a cyber range training centre to exercise emergency response, and it creates a CERT for the region.[68] Creating such an ASEAN-CERT has also been one of the ASEAN ICT Masterplan 2020 objectives.[69] The ASEAN-CERT would have less of a coordination role for CERTs since there is already substantial cooperation under APCERT, but would

[60] Cyber Security Agency Singapore (2016) 'ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN'. https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean#sthash.N2wSyXLM.h5MpHQiy.dpuf

[61] Djafar, Wahyudi (2019) 'Patchy Cybersecurity Policy in Southeast Asia', in Christian Fitriani Pareira & Naufal Armia Arifin, Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia, Centre for Strategic and International Studies.

[62] Association of Southeast Asian Nations (ASEAN) (2018) 'Leaders' Statement on Cybersecurity Cooperation Strategy'. 32nd ASEAN Summit.

[63] Association of Southeast Asian Nations (ASEAN) (2020) 'Chairman Statement'. 37th ASEAN Summit.

[64] Cybersecurity Agency Singapore (2018) 'ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts'. https://www.csa.gov.sg/news/press-releases/amcc-2018

[65] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[66] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[67] https://www.kkmm.gov.my/en/public/latest-news/17895-bernama-08-oct-2020-malaysia-presents-progress-on-norms-of-responsible-states-behaviour-in-cyberspace-at-amcc

[68] Cybersecurity Agency of Singapore (2018) 'CSA Hosts 13th Iteration of ASEAN CERT Incident Drill (ACID). https://www.csa.gov.sg/news/press-releases/sicw-2018---highlights-and-testimonials

[69] Association of Southeast Asian Nations (ASEAN) (2015) 'The ASEAN ICT Masterplan 2020'.

undertake incident response for the whole region. In parallel with the ASCCE, the AJCCBC was opened in Thailand in 2018. It trains cybersecurity workforces in governmental agencies and critical infrastructures.[70] As is understood by countries in the region, the two initiatives address cyber capacity building in a complementary rather than an overlapping manner to avoid competition.[71]

There have been resilience policy efforts in the past decade, notably culminating in a Critical Information Infrastructure Protection (CIIP) guideline for ASEAN states in 2016.[72] Malaysia defined critical national information infrastructure in its 2016 cybersecurity policy, as did the Philippines in 2017.[73] Owners of designated critical information infrastructure are only subject to cybersecurity audits in Singapore, where they are obligated to comply with specified incident reporting requirements.[74] The COVID-19 pandemic heightened attention to the significance of Critical Information Infrastructure (CII), and the 5th AMCC proposed that all relevant sectoral bodies identify areas of cooperation and capacity building in order to strengthen the cyber resilience of CIIs that are the backbone of regional communication and trade.[75]

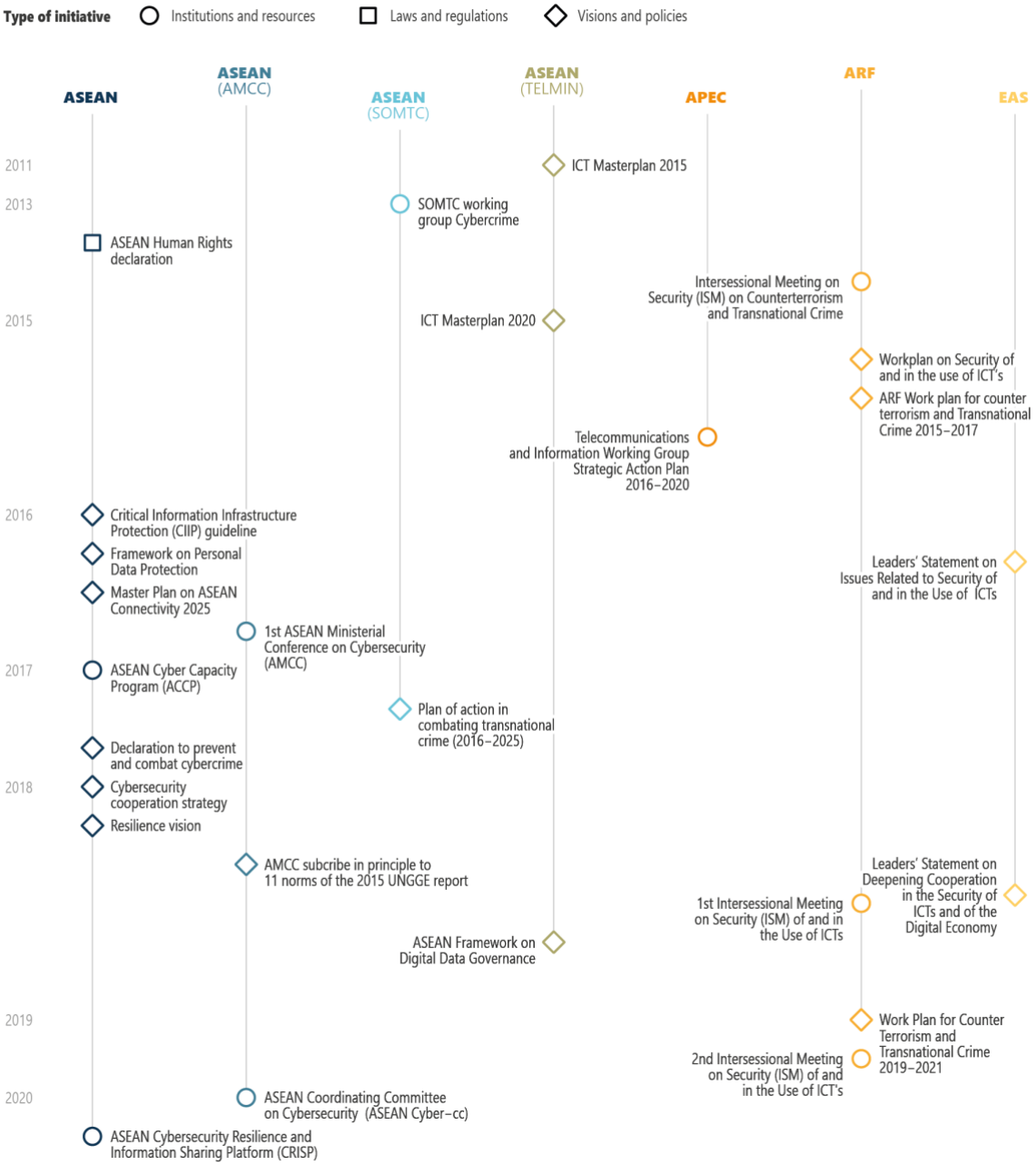
Singapore also committed itself to protecting critical infrastructures that go beyond digital services but are connected to the internet nonetheless, by launching an expert panel on operational technology in 2020. This group advises government agencies and stakeholders on strategies to enhance the resilience of their operational technology (OT) systems.[76] The CSA of Singapore also launched a Cybersecurity Labeling Scheme (CLS) in 2020 that establishes cybersecurity rating levels for connected IoT devices. The CSA plans to work with ASEAN member states to have mutual recognition arrangements for these standards across the region.[77]

In short, ASEAN is taking huge strides in improving the region's cybersecurity, creating collective resilience and protecting critical infrastructures, while taking account of differences in countries' maturity and capacity.

[70] Thai Electronic Transactions Development Agency (2018) 'MDES to Launch AJCCBC this June in Preparation for Cyber-attacks'.
[71] Noor, Elina (2018) 'ASEAN Takes a Bold Cybersecurity Step'. *The Diplomat*. https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/
[72] Association of Southeast Asian Nations (ASEAN) (2016) 'Critical Information Infrastructure Protection Guidelines'. 9th ASEAN–Japan Information Security Policy Meeting.
[73] Djafar, Wahyudi (2019) 'Patchy Cybersecurity Policy in Southeast Asia', in Christian Fitriani Pareira & Naufal Armia Arifin, Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia, Centre for Strategic and International Studies.
[74] Republic of Singapore (2018) 'Cybersecurity Act'. https://sso.agc.gov.sg/Acts-Supp/9-2018/
[75] Association of Southeast Asian Nations (ASEAN) (2020) 'Chairman Statement'. 37th ASEAN Summit.
[76] Cyber Security Agency Singapore (2020) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2020'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2020
[77] Cyber Security Agency Singapore (2020) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2020'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2020

Policy initiatives

A timeline



3.2 Confidence building

The ASEAN Regional Forum (ARF), with its mandate of preventative diplomacy, has been working on developing confidence-building measures for all ARF member states since its inception. It first noted the importance of cybersecurity in its 2012 statement on 'Cooperation on Ensuring Cyber Security'.[78] It consequently developed an ICT security workplan in 2015, with the objectives to 'avoid misperceptions,

[78] ASEAN Regional Forum (2012) 'Statement on Cooperation in Ensuring Cyber Security'. 19th ARF Ministerial Meeting.

improve cooperation to respond to criminal and terrorist use of ICTs and to cooperate to develop resilient government ICT environments'.[79]

A first workshop to operationalise CBMs for cooperation during cyber-incidence response was organised in 2016 by Malaysia and the European Union.[80] The ARF subsequently created the Inter-Sessional Meetings (ISMs) on ICT Security in 2017. The first two sessions were held in 2018 and 2019 under the co-chairing of Singapore, Malaysia and Japan, whose chairmanship ends in April 2020. An expert-level body subordinated to the ISM was created, called the Open Ended Study Group (OESG), which convenes experts to discuss CBMs to reduce the risk of conflict stemming from the use of ICTs. This has proved useful to build consensus and involve experts for in-depth debates. There have been five OESGs between 2018 and 2020, which submitted proposals to the ministerial meetings and ISMs on ICT Security. The ARF's Experts and Eminent Persons group (EEPs) also held a Working Group on ARF Initiatives in Promoting Cyber Security, and briefed the ISM in 2018.

Since its establishment, the ARF ISM on ICTs security has made incremental progress. In the 2018 ISM there were 16 proposed activities, springing from the 11 CBMs formulated in the 2015 workplan and five additional activities that were formulated at the 1st ISM on ICT security. The 1st ISM selected five CBMs for immediate activities.[81] The 3rd ISM was unfortunately not able to take place in 2020 due to the COVID-19 pandemic, and will be held at the end of April 2021.

Confidence-Building Measures	Leading Countries	Implentation Status
CBM#1: Establishing a directory of senior policy points of contact	Malaysia and Australia	Directory created
CBM#2: Voluntary sharing of information on national laws, policies, best practices and strategies	Japan and the Philippines	First country presentations made at the 2nd ISM
CBM#3: Implementation of preventive and cooperative frameworks for capacity and awareness building to protect critical infrastructures	European Union and Singapore	Ongoing
CBM#4: Awareness-raising and information sharing on emergency responses to security incidents in the use of ICTs	China, Singapore and Cambodia	Ongoing

[79] ASEAN Regional Forum (ARF) (2015) 'Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)'. http://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf

[80] Malaysia Ministry of Foreign Affairs (2016) 'ARF Workshop on Operationalising Confidence Building Measures for Cooperation during Cyber-incidence Response'. https://www.kln.gov.my/web/nzl_wellington/home/-/asset_publisher/WSOOcz6SWhzK/blog/asean-regional-forum-arf-:-workshop-on-operationalising-confidence-building-measures-for-cooperation-during-cyber-incident-response-mandarin-oriental-hotel-kuala-lumpur-from-2-3-march-2016?inheritRedirect=false

[81] Association of Southeast Asian Nations (ASEAN) (2018) 'Co-Chairs' Summary Report of the 1st ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF ISM on ICTs Security)'. http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/CO-CHAIRS-SUMMARY-REPORT-of-1st-ISM-on-ICTs-Security-FINAL.pdf

CBM #5: ARF Workshop on Principles of Building Security of and in the Use of ICTs in the National Context	Singapore and Canada	First workshop held in June 2019

CBM#1 on establishing points of contact resulted in the creation of a POC directory in 2019, for which participation was voluntary and non-binding. States with no single coordination point of contact could choose to add contacts for diplomatic, national security and policy coordination, law enforcement and technical.

CBM#2 saw its first implementation during the 2nd ISM when ARF participants shared and exchanged views on their regional and national efforts in cyber security.

For CBM#5, a workshop on building national security was organised in Singapore in 2019 together with Canada. Canada leveraged its membership in the Organisation of American States (OAS) for this workshop and invited several Latin-American countries to share their experience with the ARF member states.

For CBM#3 and CBM#4, workshops were to be organised in 2020, which were not possible due to the COVID-19 pandemic.

While the ISM has fostered renewed cooperation between major global actors that have a stake in South-East Asia, there are some obstacles to progress. Not all ARF members have the same security priorities, there is a lack of trust in the information infrastructure and there are some major differences in national perceptions regarding cyberspace threats and challenges.[82] The ISM has however been very constructive: the information sharing on national policy was a novelty for the region, showing a promising avenue to exchange perspectives.[83]

3.3 Cybercrime

According to a 2019 INTERPOL report, member countries in the ASEAN region experienced a significant amount of cybercrime, ranging from massive data breaches to crippling ransomware attacks and the meteoric rise in cryptojacking.[84,85] Cybercrime attacks also emanate from the region. In 2016 the Philippines ranked sixth in the world in web attack origins, according to a Symantec Internet Security Threat report.[86]

The Philippines seems to have improved its local threat situation, as Kaspersky found in 2019 that the number of malicious hosts in the Philippines was decreasing.[87] This seems to be the case for all South-East Asian states, which have made progress on tackling cybercrime in recent years. Every ASEAN country now has some form of cybercrime legislation according to UN observers.[88] There is serious

[82] ASEAN Regional Forum Experts and Eminent Persons (ARF/EEP) (2018) 'Recommendations for ARF Initiatives on Promoting Cyber Security'.

[83] Ministry of Foreign Affairs Japan (2019) 'ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ICTs) and 2nd ARF-ISM on ICTs Security'. https://www.mofa.go.jp/press/release/press4e_002400.html

[84] Cryptojacking is the unauthorised use of someone else's computer to mine cryptocurrency.

[85] INTERPOL (2020) 'ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk'. https://www.interpol.int/en/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf

[86] Symantec (2016) 'Internet Security Threat Report'. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-government-en.pdf

[87] Manila Standard (2020) "Kaspersky 2019 report: PH is world's 4th country with highest number of detected online threats" https://manilastandard.net/index.php/tech/tech-news/318639/kaspersky-2019-report-ph-is-world-s-4th-country-with-highest-number-of-detected-online-threats.html

[88] United Nations Conference on Trade and Development. 'Cybercrime Legislation Worldwide.' https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

cooperation on cybercrime between ASEAN member states, with a dense network of bilateral mutual legal assistance treaties. [89] Unfortunately, there is no general overarching regulation. A coordinated approach to battle cybercrime was formulated in the ASEAN plan of action in combating transnational crime (2016–2025) with an emphasis on sharing information and building capacity of law enforcement.[90]

There is serious cooperation on cybercrime between ASEAN member states, with a dense network of bilateral mutual legal assistance treaties. Unfortunately, there is no general overarching regulation.

An ASEAN extradition treaty is currently in the works, which will provide a powerful tool for the region in the fight against cybercrime.[91] In the meantime, a yearly ASEAN working group on cybercrime has been gathering since 2013 as the Senior Officials Meeting on Transnational Crime (SOMTC), to improve cooperation.[92] The ARF also developed a 2015–2017 work plan on Counter Terrorism and Transnational Crime (CTTC), which identified some means of cooperation against cybercrime and terrorist use of ICT.[93] Cybercrime is no longer part of the 2019–2021 work plan, as this issue has been placed under the previously mentioned ISM for ICTs. Preliminary discussion in the ARF's ISM on ICT Security has concluded that there was no common understanding of the definition of cybercrime yet, nor a common approach to address this issue for now.[94]

Capacity has been built through the Jakarta Centre for Law Enforcement Cooperation (JCLEC). The centre of excellence jointly owned by the Indonesian National Police (INP) and the Australian Federal Police (AFP) has existed since 2004. It has provided training to police in the region on computer forensics, cybercrime and intelligence gathering to combat transnational crime.[95]

An important international organisation for the region is INTERPOL. This international law enforcement cooperation established an ASEAN Cyber Capability Desk in 2018 to improve coordinated actions against cybercrime under the form of Joint Cybercrime Operations. Two successful operations have been executed since then.[96] It also provides ASEAN authorities with cybercrime intelligence at the strategic, operational and tactical levels through cyber activities reports. INTERPOL has also been assisting in an ASEAN Cyber Capacity Development Project (ACCDP) since 2016, which is funded by the Japan-ASEAN Integration Fund (JAIF), Singapore and the ASEAN secretariat.[97] It recently also developed a regional cybercrime strategy for ASEAN in 2019, which sets out INTERPOL's key priorities and principles in combating cybercrime in the region.[98]

[89] Chen, Qihen (2017) 'Time for ASEAN to Get Serious about Cyber Crime'. *The Diplomat.* https://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/

[90] Association of Southeast Asian Nations (ASEAN) (2017) 'ASEAN Plan of Action in Combatting Transnational Crime (2016-2025)', adopted by the 11th AMMTC.

[91] Association of Southeast Asian Nations (ASEAN) (2018) 'ASEAN Leaders' Vision for a Resilient and Innovative ASEAN'.

[92] Association of Southeast Asian Nations (ASEAN) (2014) 'ASEAN Working Group on Cybercrime: Terms of Reference'. https://asean.org/storage/2018/01/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf

[93] ASEAN Regional Forum (ARF) (2015) '2015–2017 ARF Work Plan for Counter Terrorism and Transnational Crime'.

[94] ASEAN Regional Forum (ARF) (2019) 'Co-Chairs' Summary Report of the 2nd ARF ISM on ICTs Security Singapore', 28–29 March 2019.

[95] Australian Department of Foreign Affairs (2019) 'Cybercrime Law Enforcement and Prosecution Capacity Building in the Indo-Pacific' from Australia's International Cyber Engagement Strategy. https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_3_cybercrime.html

[96] Operation Goldfish Alpha against Cryptojacking Led to a Reduction of Infected Routers by 78 Per Cent, and Operation Night Fury against Malware Targeting E-Commerce Websites Saw the Arrest of Three Individuals Suspected of Controlling Command Servers in Indonesia. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

[97] INTERPOL (2020) ASEAN Cyber Capacity Development Project. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-training-for-police/ASEAN-Cyber-Capacity-Development-Project-ACCDP

[98] INTERPOL (2020) 'ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk'. https://www.interpol.int/en/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf

The Philippines has also taken significant steps to improve its capacities on cybercrime, partly with the support of the European Union and the Council of Europe through the Global Action on Cybercrime (GLACY+) project. In 2018, the Philippines became the first ASEAN state to adopt the Budapest Convention. The country has been at the forefront in the region in terms of creating awareness for states to also accede to the convention.

Most countries, however, are not keen on adopting the Budapest Convention, sometimes led by the argument that they had no part in creating it.[99]

3.4 Freedom of expression online

Cybercrime legislation in some South-East Asian countries has extended to the online sphere. Thailand's 2016 Computer-Related Crime Act, for instance, grants the government the authority to restrict freedom of speech and expression, stretching the concept of 'cybercrime' far beyond ICT intrusions. Vietnam's cybercrime law also extends far beyond technology issues, and is accompanied by a 10,000-strong cyber unit that identifies and counters 'wrongful opinions' critical of the one-party government.[100]

Criminalisation of online content is mostly framed as a cybercrime matter. Many ASEAN states' cybercrime policy is focused more on avoiding social disruption and controlling the spread of disinformation than on technology issues.

ASEAN states such as Laos, Singapore and Indonesia have introduced legal provisions in the past few years that criminalise content categorised as 'fake news'. Malaysia, fortunately, revoked its 2018 Anti-Fake News Act when its content was considered to restrict freedom of speech and expression, and is one of the few countries reversing this trend.[101] Thailand, Laos, Cambodia, Myanmar, Brunei and Vietnam still have antidefamation laws in place that extend to online expression. This criminalisation of online content is mostly framed as a cybercrime matter. Many ASEAN states' cybercrime policy is focused more on avoiding social disruption and controlling the spread of disinformation than on technology issues.[102]

These are all worrying signs for the freedom and openness of the internet, as they cause strong self-censorship behaviour by social media users. Several international digital rights organisations have deemed the measures to infringe human rights principles of freedom of expression.[103] In 2019, Freedom House categorised Vietnam, Cambodia, Laos, Myanmar and Brunei as 'not free', and all other ASEAN states as only 'partly free', in its yearly 'freedom of the net' report.[104] Thailand seemed to be climbing from 'not free' to partly free in 2020, as it was ending a period of direct rule by military commanders and appeared to be reducing its restrictions on public assembly. There are also civil society recommendations to the Thai government to create a human-centred Cybersecurity Act that protects

[99] Australian Strategic Policy Institute (2015) 'Cyber Maturity: ASPI 2015 Report'.

[100] Hookway, James (2017) 'Introducing Force 47, Vietnam's New Weapon against Online Dissent'. https://www.wsj.com/articles/introducing-force-47-vietnams-new-weapon-against-online-dissent-1514721606

[101] Djafar, Wahyudi (2019) 'Patchy Cybersecurity Policy in Southeast Asia', in Christian Fitriani Pareira & Naufal Armia Arifin, *Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia*, Centre for Strategic and International Studies.

[102] Ang, Benjamin (2020) 'Singapore, ASEAN and International Cybersecurity', in Eneken Tikk & Mika Kerttunen, *Routledge Handbook of International Cybersecurity*, Routledge.

[103] The International Commission of Jurists compiled analyses and reports of digital rights organisations on South-East Asia in the 2019 report 'Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia'. https://www.icj.org/wp-content/uploads/2019/12/Southeast-Asia-Dictating-the-Internet-Publications-Reports-Thematic-reports-2019-ENG.pdf

[104] Freedom House (2019) 'Freedom on the Net 2019 Report'. https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

online freedom and privacy while tackling cyber threats. This initiative, the first of its kind, is promising to create more rights-centric policy on a national level.[105]

For now, there are still many disturbing trends for digital rights in the region. There have been frequent internet shutdowns, serving as a tool for control during times of social unrest or elections. The most notable of these in 2019 happened in Indonesia during presidential elections. The government enforced a 78-hour social media shutdown across the country after riots erupted in Jakarta and New Guinea.[106]

Disinformation has also been used by governments in South-East Asia against political adversaries, for example by Philippines president Duterte in 2017, and against him in 2019.[107] This type of abuse became problematic in Myanmar in 2018, where a UN fact-finding mission found the government guilty of spreading hate speech on social media, which significantly contributed to the genocide against the Rohingya in the country.[108]

ASEAN leaders adopted a joint declaration in 2017 promoting a culture of prevention for a peaceful, inclusive, resilient, healthy and harmonious society to prevent deliberate falsehoods and counter violent extremism.[109] While they affirmed compliance with human rights, they have different interpretations and approaches in applying the preventative principles in their own countries when it comes to the online space, and there is no enforcement mechanism to make states comply with these principles. There have, however, been efforts by the ASEAN ministers responsible for information to tackle the harmful effects of fake news, which culminated in a 2018 framework and declaration on fake news and digital literacy that supports civil society involvement.[110]

3.5 Digital economy

The Economic Research Institute for ASEAN and East Asia (ERIA) has projected that the ASEAN digital economy will expand by a factor of more than six in the next decade, to an estimated US$200 billion.[111] The digital economy has long been a priority for ASEAN for the development of its societies. Digital transformation initiatives were set up in the early 2000s, such as the 2000 e-ASEAN Framework Agreement, which aimed to develop the electronic infrastructure for commerce in the region; and the 2003 Singapore Declaration, which emphasised the need to establish an interoperable ASEAN information infrastructure. ASEAN has been consistently working on improving the connectivity of the region, for example through its ASEAN ICT Masterplan (AIM) created in 2011 and 2015 with a five-year horizon, the new ASEAN Digital Masterplan 2025 and the Masterplan on Connectivity for 2025.[112]

---

[105] Manushya Foundation (2019) 'Thailand's Cybersecurity Act: Towards a Human Centered Act Protecting Online Freedom and Privacy, While Tackling Cyber Threats'. https://www.manushyafoundation.org/study-on-cybersecurity-act

[106] Louis, Jillian (2020) 'Internet shutdowns could cost ASEAN dearly'. https://theaseanpost.com/article/internet-shutdowns-could-cost-asean-dearly

[107] Palatino, Mong (2017) 'Beware Duterte's Troll Army in the Philippines'. *The Diplomat*, https://thediplomat.com/2017/11/beware-dutertes-troll-army-in-the-philippines/

Samantha Bradshaw & Philip N. Howard (2019) 'The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.' Working Paper 2019.3. Oxford, UK: Project on Computational Propaganda.

[108] United Nations High Commissioner for Human Rights (2018) 'Report of the Independent International Fact-Finding Mission on Myanmar'. Human Rights Council, A/HRC/39/64.

[109] Association of Southeast Asian Nations (2017) 'ASEAN Declaration on Culture of Prevention for a Peaceful, Inclusive, Resilient, Healthy and Harmonious Society'. 31st ASEAN Summit.

[110] Association of Southeast Asian Nations (2018) 'Framework and Joint Declaration to Minimise the Harmful Effects of Fake News'. 14th Conference of the ASEAN Ministers Responsible for Information (AMRI).

[111] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[112] Association of Southeast Asian Nations (2011) ASEAN ICT Masterplan 2015. http://www.asean.org/storage/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf

ASEAN ICT Masterplan 2020. https://www.trc.gov.kh/wp-content/uploads/2016/10/1.pdf

ASEAN Digital Masterplan 2025. https://asean.org/storage/ASEAN-Digital-Masterplan-2025.pdf

ASEAN Masterplan for Connectivity 2025. https://asean.org/wp-content/uploads/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf

While there is a big push from the more technologically advanced states such as Singapore to integrate the market into a single digital market, the question remains whether these aspirations are feasible given the digital divide of the region in terms of maturity. Some countries also create barriers for cross-border data flows, such as Indonesia, Malaysia and Vietnam, whose data protection regulations require data about their citizens to be stored on local servers.[113]

Nonetheless, there is an intention in ASEAN to build a digital single market. An ASEAN digital integration framework will monitor the progress of its digital integration, an initiative that is still being developed.[114] There is great interest by South-East Asian countries in the EU's approach and experience in digital economy and connectivity, which has resulted in knowledge exchanges on the EU's digital Single Market completion.[115]

The overarching development to support such a digital integration would need a digital data governance framework, as mentioned in the ASEAN Masterplan on Connectivity 2025.[116] Such a framework should aim to strengthen digital data collection and management capabilities of businesses across the region, and engender trust in businesses' data collection and management practices. The TELMIN endorsed such a framework in December 2018 and tasked the senior officials to further develop and implement initiatives under the framework.[117] Creating a single digital market requires a safe and trusted ICT environment in ASEAN, which is also one of the desired outcomes of the Digital Masterplan 2025. Ensuring that cybersecurity and digital data governance best practices are adopted as widely as possible should increase trust in digital services and prevent consumer harm.[118]

Countries that are part of APEC[119] also understood the need to include cybersecurity in the trade organisation's digital strategy to create a secure, resilient and trusted ICT environment. APEC countries intend to create an APEC Framework for Securing the Digital Economy.[120] For now, such ambitions are mostly hindered by a lack of sector-specific governance on cybersecurity. The financial sector has a mature governance structure and a Financial Services Information Sharing and Analysis Center (FS-ISAC) for the region: this sector is the pioneer in the region.[121] Sector-specific governance is low on regional cooperation agendas, but is essential to protect a digital single market.

Apart from regulatory stumbling blocks and synergy problems in unifying the market, a possible hindrance to the digital economy is the fallout of the US–China trade war. This can impact digital development, innovation and, ultimately, security. The US has become very focused on reducing China's influence on the region by taking a tough stance on trade and Chinese intellectual property (IP) theft.

---

[113] Basu Das, Sanchita (2018) 'An ASEAN Digital Market? Small Beginnings, Great Endings'. ISEAS Yusof Ishak Institute. https://www.iseas.edu.sg/medias/commentaries/item/7102-to-an-asean-single-digital-market-small-beginnings-great-endings-by-sanchita-basu-das

[114] Association of Southeast Asian Nations (ASEAN) (2018) 'Chairman Statement'. 33rd ASEAN Summit.

[115] European Commission (2019) 'The EU and ASEAN: Building Stronger Digital Economy & Connectivity Cooperation'. Event report. https://ec.europa.eu/digital-single-market/en/news/eu-and-asean-building-stronger-digital-economy-connectivity-cooperation

[116] Master Plan on ASEAN Connectivity 2025. https://asean.org/wp-content/uploads/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf

[117] The 18th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings, Bali, Indonesia, 6 December 2018: Joint Media Statement. https://asean.org/storage/2018/12/TELMIN-18-JMS_adopted.pdf

[118] Master Plan on ASEAN Connectivity 2025. https://asean.org/wp-content/uploads/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf

[119] Members: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Vietnam.

[120] Asia-Pacific Economic Cooperation (APEC) 'Telecommunications and Information Working Group', last accessed 18/03/2019. https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

[121] Marsh & McLennan Companies (2017) 'Cyber Risk in Asia-Pacific: The Case for Greater Transparency'. Asia Pacific Risk Center

[122] While the resistance to IP theft is welcomed by countries in the region, they are also cautious regarding the US approach on trade. A severe slowdown in Chinese economic growth could have dire consequences for countries whose digital development hinges on Chinese manufacturing.[123]

There has been some movement to reduce this dependency. Countries in the region such as Brunei, Malaysia, Singapore and Vietnam that wished to build an economic space across the Pacific without involving China entered the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) in 2018. The partnership created one of the largest free-trade zones, with 11 countries across the Pacific, strengthening ties between Asia and Latin America.[124] It was almost dead in the water when the US left it in 2017, but was revived by Japan and other regional actors. The CPTPP includes a clause on non-discriminatory treatment of its digital products to avoid trade-war-like outcomes, creating stability for a region that is in the middle of this dynamic.[125]

[122] Ford, Linsey (2019) 'Free, Open and Sharper-Edged: America's Embrace of Strategic Competition'. CSCAP Regional Security Outlook 2019.
[123] Ibid.
[124] Asia Perspective (2019) 'Building Commercial Links Between Asia and Latin America – The Trans-Pacific Partnership'. http://asiaperspective.net/2019/06/12/building-commercial-links-asia-latin-america-trans-pacific-partnership/
[125] Comprehensive and Progressive Trans-Pacific Partnership (2018) 'Chapter 14: Electronic Commerce'. https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf

4 Regional approaches to cyber diplomacy and resilience

Cyber diplomacy can be interpreted as the use of diplomatic means to create stability in cyberspace. While ASEAN has not formally developed a cyber diplomacy strategy, the South-East Asian countries are highly shaped by their position between great powers that have wildly different approaches to regulating cyberspace. Between China and Russia's push for sovereignty over internet borders and the US and other Western countries' push for multi-stakeholder governance of the internet, ASEAN states have managed to carve out a middle ground that follows the standing consensus on international law and norms. ASEAN seems to be pushing the envelope on furthering the process of implementation of norms and application of international law by being the first region in the world that has adopted the 2015 UNGGE norms on responsible state behaviour in cyberspace.

Until a few years ago, there was no serious participation of ASEAN in the conversation on international rules on responsible state behaviour in cyberspace. Only Malaysia, Indonesia and Singapore previously participated in the UNGGE. This grew in 2017, when states pledged to form global consensus on norms on cyberspace in an ASEAN statement to the United Nations, which was presented by Singapore.[126] The ASEAN ministers for cybersecurity in the AMCC had been tasked to develop a set of practical cybersecurity norms of state behaviour for ASEAN. They agreed at the third AMCC in 2018 to subscribe in principle to the 11 voluntary, non-binding norms set out in the 2015 report by the UNGGE, instead of developing new norms.[127] The work of the UNGGE was also recognised in the ARF 2015 ICT work plan, with 'no intention to duplicate the work'.[128] No further mention of the UNGGE norms has been made in ARF circles, as its mandate focuses primarily on CBMs.

> **ASEAN states agreed in 2018 to subscribe in principle to the 11 voluntary, non-binding norms set out in the 2015 report by the UNGGE, instead of developing new norms.**

At the 2019 AMCC, member states agreed to establish a working-level committee to develop a long-term regional action plan for the practical implementation on the UNGGE norms, as previously discussed.[129] The Singaporean minister of cybersecurity called on ASEAN member states in the 2019 AMCC to participate in international discussions to demonstrate ASEAN's thought leadership, and ensure that the region's interests and context are taken into account.[130]

How exactly ASEAN member states will observe the norms they have adopted when actual incidents occur is as yet unclear. ASEAN states have so far refrained from 'naming and shaming' as they lack the means to accurately attribute the true source of cyberattacks, and the risk of a wrong attribution is high.[131] Apart from a general statement that international law is applicable in cyberspace, the region's perception of the application of international law is prominently lacking. It is also not clear how states

[126] Singapore Ministry of Foreign Affairs (2017) 'Statement on Behalf of the Members of Southeast Asian Nations at the Thematic Debate on Cluster 5: Other Disarmament Measures and International Security of the First Committee'. https://www.mfa.gov.sg/Overseas-Mission/New-York/Mission-Updates/First_committee/2017/10/press_20171023

[127] Cybersecurity Agency Singapore (2018) 'ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts'. https://www.csa.gov.sg/news/press-releases/amcc-2018

[128] ASEAN Regional Forum (ARF) (2015) 'Workplan on Security of and in the Use of Information and Communications Technologies (ICTs)'.

[129] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[130] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[131] Raska, Michael & Ang, Benjamin (2018) 'Cybersecurity in Southeast Asia', introductory note to the roundtable on 22 May 2018, Southeast Asia Observatory. https://centreasia.eu/en/cybersecurity-in-southeast-asia-benjamin-ang-dr-michael-raska-2/

in the region intend to 'guarantee full respect for human rights, including the right to freedom of expression' when dealing with online content that threatens to destabilise and undermine political stability, as there have been some concerning trends towards criminalisation of online content. [132] The working-level committee could potentially bring clarity on these missing issues. However, Ang argues that ASEAN states would do best to limit the scope of the regional and international discussion on cyberspace stability to technology issues. It would be better to leave strategies for managing content out of this discussion, and up to individual strategies domestically. This would avoid ideological disagreements and allow effective cooperation.[133]

Russia and China developed their own position in the international debate under the auspices of the Shanghai Cooperation Organisation (SCO), where they created a code of conduct for information security. This code of conduct mainly focused on respect for sovereignty and territorial integrity of states in the information space.[134] Russia and China submitted this code to the UN in 2011[135] and 2015;[136] it called for an alternative working mechanism within the framework of the UN. A lot of the SCO code of conduct's language was usued in a UN proposal for an Open Ended Working Group (OEWG). [137] All ASEAN states voted for an OEWG UN proposal in 2018 that would expand the discussion on peace and security in cyberspace to the whole UN membership. Almost all ASEAN states also voted in the same year for a UN proposal that would continue the UNGGE process with a smaller participation.[138] Only Cambodia, Lao and Myanmar abstained. The representatives from Singapore, the Philippines, Indonesia and Malaysia stated at the UN that the processes to be established by the two drafts are not incompatible. They called for a depoliticised process.[139] At the UNGGE chair's regional consultation with ASEAN member states, states expressed a clear preference for a rule-based order enforced through UN processes.[140]

For the continuation of the UN processes on acceptable state behaviour in cyberspace, two competing proposals were approved in 2020: most ASEAN states voted for both tracks, except that Cambodia, Laos and Myanmar abstained from voting for the US-sponsored resolution to await the decision of the UNGGE and UNGA on the continuation of the cybersecurity processes.[141]

This support for both UN processes is indicative of ASEAN's central position that it has adopted as a bridging role. As Krisetya argues, ASEAN tries not to succumb to the choice between exclusive state-centric cybersecurity governance and an unsupervised, market-based multi-stakeholder approach, but

[132] Noor, Elina (2018) 'ASEAN takes a bold cybersecurity step'. *The Diplomat*, https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/

[133] Ang, Benjamin (2020) 'Singapore, ASEAN and international cybersecurity', in Eneken Tikk & Mika Kerttunen, *Routledge Handbook of International Cybersecurity*, Routledge.

[134] UN General Assembly (2015) 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General'. https://digitallibrary.un.org/record/786846?ln=en

[135] UN General Assembly (2011) 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General'. https://digitallibrary.un.org/record/710973?ln=en

[136] UN General Assembly (2015) 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General'. https://digitallibrary.un.org/record/786846?ln=en

[137] UN General Assembly (2018) 'Developments in the Field of Information and Telecommunications in the Context of International Security'. A/RES/73/27. https://undocs.org/A/RES/73/27

[138] UN General Assembly (2018) 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. A/RES/73/266. https://undocs.org/A/RES/73/266

[139] United Nations (2018) 'First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct'. First Committee, GA/DIS/3619. https://www.un.org/press/en/2018/gadis3619.doc.htm

[140] United Nations Office of Disarmament Affairs (2019) 'Collated Summaries of the Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf

[141] Russia proposal. https://undocs.org/en/A/C.1/75/L.8/Rev.1US proposal. https://undocs.org/en/A/C.1/75/L.4

elects to be a 'broker' between the Chinese and US styles of cybersecurity governance.[142] This is also reflected in the participation of ASEAN states in the Paris Call for stability in cyberspace, which observers put forward as a 'third way' to govern the internet.[143] Cambodia, The Philippines and Singapore signed onto the Paris Call, as well as non-state actors in Indonesia, Malaysia, Thailand and Vietnam.[144] At the opening of the 4th AMCC, the Paris Peace Forum where the Paris Call was launched, as well as the UNGGE and OEWG, was mentioned as a key forum for discussions on international cyber norms and standards.[145]

> **ASEAN tries not to succumb to the choice between exclusive state-centric cybersecurity governance and an unsupervised, market-based multi-stakeholder approach, but elects to be a 'broker' between the Chinese and US styles of cybersecurity governance.**

As acceptable state behaviour in cyberspace also assumes due diligence, the international conversation has started moving towards developing more consensus on cybercrime. A new resolution for the creation of a multilateral framework on cybercrime was advanced in the UN Third Committee by Russia and China. This resolution raised some serious human rights concerns, as its vagueness could open the door to criminalising online behaviour that is protected under International human rights law.[146] It also established a competing process to the UN Intergovernmental Expert Group on Cybercrime (IEG), which was established in 2010, as the new resolution demands the establishment of an Open-Ended Ad Hoc Intergovernmental Committee of Experts to elaborate a comprehensive international convention on 'countering the use of information and communications technologies for criminal purposes'. The first organisational session of the open-ended committee was postponed in 2020 due to the COVID-19 pandemic.[147]

All ASEAN member states except for the Philippines (which has acceded to the Budapest Convention) voted for the 2019 UN proposal on countering the use of ICT for criminal purposes. Their vote for the new UN proposal can be seen as a demand to be included in the creation of an international framework, as they were not involved in the creation of the Budapest Convention at the time. Little comment was made by South-East Asian states at the 2018 vote when it was first introduced.[148] At the 2019 vote, Indonesia expressed support for the initiative, and called for politicisation to be avoided and best practices from existing initiatives to be used.[149]

---

[142] Krisetya, Beltsazar 'Examining Southeast Asia's Cyber Terrain', in Christian Fitriani Pareira & Naufal Armia Arifin, Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia, Centre for Strategic and International Studies.

[143] Laudrain, Arthur P.B. (2018) 'Avoiding a World War Web: The Paris Call for Trust and Security in Cyberspace'. Lawfare Blog. https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace

[144] France Ministry for Europe and Foreign Affairs (2018) 'Paris Call of 12 November 2018 for Trust and Security in Cyberspace' https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[145] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[146] 'Open letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online'. https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf

[147] Ad Hoc Committee Established by General Assembly Resolution 74/247. https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[148] United Nations (2018) 'Third Committee Approves 11 Drafts amid Heated Debate over Death Penalty Moratorium, Use of Mercenaries, Efforts to End Cybercrime'. Third Committee, GA/SHC/4252. https://www.un.org/press/en/2018/gashc4252.doc.htm

[149] 'Third Committee Passes 15 Draft Resolutions on Child Rights, Rural Women, with Divisions over Sexual, Reproductive Health Care Chipping Away at Consensus'. https://www.un.org/press/en/2019/gashc4284.doc.htm

5 International engagement

South-East Asia is a crowded space with conflicting perspectives. There are struggles for alliances, most prominently by the Chinese and US powers, and a long history of cooperation with other actors in the region such as Japan, Korea and Australia. Russia also participates in the region, increasingly in tandem with China, and the EU is currently seen as the most trusted partner. According to some scholars, ASEAN states seem to have evolved from rejecting great power competition in the region, to accepting the region's centrality on these issues.[150] The relationship with the key players in the region is explored in this chapter.

5.1 The US and China

The US has a complicated history with South-East Asia. It colonised the Philippines at the start of the 20th century and later pressed European colonialists to dismantle their empires in South-East Asia. American efforts during the Cold War to stop South-East Asian states from turning into communist regimes, and to 'topple the dominos' of Soviet and Chinese influence, led to the Vietnam war. The US has always seen the significance of South-East Asia for geopolitics and global security, and was previously called a stabilising force in the region by former Prime Minister of Singapore Goh Chok Tong.[151] After the Vietnam war, it built its policy on maintaining a strong strategic and cooperative military relationship with ASEAN countries.[152] The bilateral ties run deepest with the Philippines due to the colonial history, and it has bilateral collective security treaties in South-East Asia with Thailand and the Philippines.[153]

The US also has major economic influence, since US companies are crucial to ASEAN's integration into regional and global supply chains.[154] The strong US economic presence has a strategic weight in counterbalancing China.[155] The US is, however, no longer perceived to be a stabilising security actor in South-East Asia. According to a 2020 survey of regional experts and policy influencers by the ASEAN Studies Centre at the Singaporean ISEAS-Yusof Ishak Institute, 47% of respondents had little or no confidence in the US as a strategic partner and provider of regional security.[156] Only 30% had confidence that the United States will 'do the right thing' to contribute to global peace, security, prosperity and governance. Just under a quarter expressed confidence in the US as the country most likely to provide leadership to maintain the rules-based order and uphold international law.[157] Also, there was very little attention to the rise of authoritarianism and illiberalism in ASEAN countries under the Trump administration, creating a vacuum for online human rights protection.[158]

The lack of US senior government officials at the East Asia Summits fuelled concern that the region is not on the US radar. The US's withdrawal from the Trans-Pacific Partnership (TPP) did not engender trust or goodwill.[159] While the presidency of Joe Biden can change the tone of the conversation, it is

[150] Amitav Acharya (2017), 'The Myth of ASEAN Centrality?', *Contemporary Southeast Asia*, 39, no. 2, p. 273.
[151] Goh Chok Tong (2000) 'Prime Minister of Singapore Speech on ASEAN–US Challenges'. https://asiasociety.org/asean-us-relations-challenges
[152] Goyer, John (2020) 'US Must Recapture Lost Ground in Southeast Asia or Risk Being Shut Out'. *The Diplomat*, https://thediplomat.com/2020/02/us-must-recapture-lost-ground-in-southeast-asia-or-risk-being-shut-out/
[153] Parameswaran, Prashanth (2017) 'Oldest US Ally in Asia: Thailand or the Philippines?' *The Diplomat*, https://thediplomat.com/2017/02/which-country-is-the-oldest-us-ally-in-asia/
[154] Ibid. 152
[155] ibid.
[156] Tang, S.M. et al. (2020) 'The state of Southeast Asia: 2020'. ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf
[157] Tang, S.M. et al. (2020) 'The State of Southeast Asia: 2020'. ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf
[158] Ford, Linsey (2019) 'Free, Open and Sharper-Edged: America's Embrace of Strategic Competition'. CSCAP Regional Security Outlook.
[159] Goyer, John (2020) 'US Must Recapture Lost Ground in Southeast Asia or Risk Being Shut Out'. *The Diplomat*, https://thediplomat.com/2020/02/us-must-recapture-lost-ground-in-southeast-asia-or-risk-being-shut-out/

unlikely that Biden will revive such a free trade agreement with the Asia-Pacific region due to domestic politics.[160] Respondents in the ISEAS survey had more confidence in China than in the US when asked which country would provide leadership in championing the global free trade agenda.

There appeared to be a shift in focus away from the US among South-East Asian nations during the Trump administration, but this did not necessarily entail a rapprochement with China. Tensions over the South China Sea are still a cause for distrust of China as a regional security provider. Fears exist that China will limit freedom of navigation in regional waters, and a mere 6% of regional experts see China as maintaining the rules-based order and upholding international law.[161] China has called for the creation of a new security architecture in Asia in the past few decades. This regional security architecture is promoted as a 'new type of security partnership' that would not be based on any alliance system but rather on a network of partnerships.[162] China's move can be seen as a means to avoid a stronger security alliance forming out of the 'Quad' of India, Japan, the US and Australia. An Indo-Pacific strategy emerged from the states that are members of this Quad, calling for a 'free and open Indo-Pacific'. This aims to counterbalance China's dominance in the South China Sea.[163] While the Indo-Pacific strategy was a laudable effort from the Trump administration that Biden has confirmed will continue, the concept is not clear for everyone, and some observers even see it as a move to undermine ASEAN's relevance.[164]

Throughout its history it has become clear that South-East Asia cannot and does not want to choose between the US and China, and a perceived push towards choosing causes unease in the region.

As long as China welcomes the overlap of security ties, this should not drastically impact the precarious balancing act of the South-East-Asian states. The hard-edged rhetoric of the Trump administration, however, created the perception of a choice between the two, a course that will be maintained by Biden.[165] Throughout its history it has become clear that South-East Asia cannot and does not want to choose between the US and China, and a perceived push towards choosing causes unease in the region.[166] Increased competition between the two countries does not have to be disadvantageous. The US–China trade war, for example, can have a positive effect for South-East Asia if production shifts from China to other countries in the region.[167] Of the ISEAS survey respondents, however, 35.9% believe that their economy has suffered from the trade war in the short term, while 28% believe that the economic repercussions of the trade war will be enduring.[168]

[160] Narine, Shaun (2018) 'US Domestic Politics and America's Withdrawal from the Trans-Pacific Partnership: Implications for Southeast Asia'. *Contemporary Southeast Asia*, Vol. 40, No. 1.

[161] Tang, S.M. et al. (2020) 'The State of Southeast Asia: 2020'. ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf

[162] Ekman, Alice (2019) 'China's "New Type of Security Partnership" in Asia And Beyond: A Challenge to the Alliance System and the "Indo-Pacific" Strategy'. Elcano Royal Institute. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari35-2019-ekmanalice-china-security-partnership-asia-and-beyond-challenge-aliance-system

[163] Pesjova, Eva (2018) 'The Indo-Pacific, a Passage to Europe?' *EUISS Brief*, 3-2018. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20The%20Indo-Pacific_0.pdf

[164] Tang, S.M. et al. (2020) 'The state of Southeast Asia: 2020'. ISEAS-Yusof Ishak Institute https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf

[165] Patil, Uday (2021) 'Joe Biden, China and the Indo-Pacific'. *Diplomatist*, https://diplomatist.com/2021/02/10/joe-biden-china-and-the-indo-pacific/

[166] Stromseth, Jonathan (2019) 'Don't Make Us Choose: Southeast Asia in the Throes of US-China Rivalry', https://www.brookings.edu/research/dont-make-us-choose-southeast-asia-in-the-throes-of-us-china-rivalry/

[167] Ford, Linsey (2019) 'Free, Open and Sharper-Edged: America's Embrace of Strategic Competition'. CSCAP Regional Security Outlook 2019.

[168] Tang, S.M. et al. (2020) 'The State of Southeast Asia: 2020.' ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf

This power struggle doesn't have a negative impact on engagements on cyberspace issues yet. Both countries are engaging with the region in improving the digital economy and building cybersecurity capacity. China has significantly invested and provided capital for development and economic growth to countries in the region under the Belt and Road Initiative, promising to enhance digital connectivity. Work on the 'digital silk road' is currently mostly carried out by China's tech companies. For example, Huawei Marine is building submarine cable projects in Indonesia and the Philippines. Huawei is also working with the Myanmar Ministry of Transport and Communications to launch 5G broadband services by 2025. Alibaba is investing in the Singapore post, a traditional postal service, to join the digital revolution, and Tencent invested in Grab, a leading ride-hailing service in South-East Asia.[169] Chinese companies are also known to work on co-ownership with local companies to retain and benefit from local brand identities.[170]

This development of the 'information infrastructure' in emerging countries is part of the Chinese International Strategy of Cooperation on Cyberspace.[171] While these efforts open up markets for developing economies, they challenge the competitive advantages of developed economies in the region. South-East Asian states that accept capacity building by China risk reducing their sovereignty when Chinese investment comes with a price in the form of 'debt-trap diplomacy'.[172]

Chinese engagement serves the purpose of 'Cultural Exchanges', as stated in its international strategy on cyberspace. These exchanges can have some normative consequences. For example Vietnam's new cybersecurity law mirrors some of China's cybersecurity laws, specifically on content control.[173] Cambodia and Laos have also been seen to choose partnership with China over maintaining consensus with their ASEAN family after receiving heavy investments. [174] Myanmar's new leaders even installed new hardware and software to enable surveillance after the 2021 coup, reportedly with Chinese help.[175] There is thus an element of Chinese strategic influence expansion when China shares its governance experience with other countries.[176] This expansion is captured in China's renewed 2018–2022 memorandum of understanding (MoU) with ASEAN, which includes information exchange, cooperation and capacity building for network security emergency response. This is also detailed in the recent 2019 ASEAN–China ICT Work Plan.

China's efforts on digital developments and cybersecurity capacity building have been paralleled by American efforts. The US signed an MoU on cybersecurity cooperation with Singapore in 2016, and built on this with a declaration of intent in 2018 for a cybersecurity technical Assistance programme for the ASEAN states. The US intends to give capacity-building workshops and exchange knowledge on the development of cybersecurity strategies.[177] Policy initiatives are detailed in the broader ASEAN–US 2019 ICT Work Plan, where structured cooperation is planned in the areas of digital economy and cybersecurity. This is in line with the Indo-Pacific strategy launched under the Trump administration.

[169] Jia Hao, Chan (2019) 'China's Digital Silk Road: A Game Changer for Asian Economies'. *The Diplomat*, https://thediplomat.com/2019/04/chinas-digital-silk-road-a-game-changer-for-asian-economies/

[170] 'Southeast Asia in the Global Digital War.' https://directionsblog.eu/southeast-asia-in-the-global-digital-war/

[171] 'International Strategy of Cooperation on Cyberspace.' http://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm

[172] Pesjova, Eva (2018) 'The Indo-Pacific: A Passage to Europe?'. EUISS Brief 3-2018. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20The%20Indo-Pacific_0.pdf

[173] Nguyen, Thoi (2019) 'Vietnam's Controversial Cybersecurity Law Spells Tough Times for Activists', The Diplomat, https://thediplomat.com/2019/01/vietnams-controversial-cybersecurity-law-spells-tough-times-for-activists/

[174] Son, Johanna (2017) 'Laos and Cambodia, the China Dance'. Myanmar Times. https://www.mmtimes.com/news/laos-and-cambodia-china-dance.html

[175] VOA Burmese service (2021) 'Burmese Expert: China Helping Military Establish Cyber Firewall ' https://www.voanews.com/east-asia-pacific/burmese-expert-china-helping-military-establish-cyber-firewall

[176] Yang Jiechi (2017) 'Study and Implement General Secretary Xi Jinping's Thought on Diplomacy in a Deep-Going Way and Keep Writing New Chapters of Major-Country Diplomacy with Distinctive Chinese Features', Xinhua, 17 July.

[177] Cybersecurity Agency Singapore (2018) 'Singapore and the United States Sign Declaration of Intent on Cybersecurity Technical Assistance Program'. https://www.csa.gov.sg/news/press-releases/singapore-and-the-us-sign-doi-on-cybersecurity-technical-assistance-programme

This will also have a focus on the digital economy, aside from other needs such as energy and infrastructure.[178]

While both countries appear to be creating a sphere of influence through economic statecraft, with varying degrees of success among ASEAN states, ASEAN appears to be managing internal cohesion well. Members seem to agree that a united and strong ASEAN is a prerequisite for the regional organisation to maintain its autonomy and to avoid entanglement with either major power.[179]

5.2 Russia

Russian involvement in the region is catalysed through its cooperation with China. Fuelled by the US–China trade war, this cooperation has seen Russia 'get ahead' using Chinese high-tech enterprises as allies, and escape its technologically disadvantaged position. There is, however indication that Russia is equally wary of potential security risks in cooperating with Huawei to build out 5G infrastructure, but is forced to rely on them in the absence of better options.[180] Prime minister Medvedev recently called upon cooperation with ASEAN states to 'de-monopolise' the high-tech industry, indicating the unease of China's dominance.[181]

Russia is increasingly involved in South-East Asia, including in security and defence matters, even if cooperation is at an early stage. It has had some loosely coordinated workshops in Moscow for some South-East Asian countries and made a joint statement with the region on cybersecurity.[182] In the statement, both regions stressed the importance of sovereignty and non-interference in internal affairs, and acknowledged the importance of adopting the norms and principles of responsible state behaviour in cyberspace. They also mutually stressed the importance of preserving the internet as an instrument of peace and development and to prevent its use as a weapon.[183] They agreed in 2020 on specific actions to promote cooperation on ICT security in the new Comprehensive Plan of Action for 2021–2025.[184]

5.3 Japan, Korea, Australia

There has been strong regional cybersecurity engagement with ASEAN by Japan, Korea and Australia. Japan has assisted ASEAN in various areas of cooperation, and has pursued activities to build technical capacities and capacities to support norms and CBMs. It co-chaired the first two successful ARF ISMs on ICTs to develop CBMs together with Singapore and Malaysia. The recent establishment of the ASEAN–Japan capacity centre based in Bangkok is another notable engagement effort. The ASEAN–Japan 2019 ICT Workplan includes the implementation of the ASEAN ICT masterplan's strategic thrusts, specifically on digitalisation. Japan's drive for capacity building in the region is included in its own cybersecurity strategy, which also includes the objective of contributing to the peace and stability of the

[178] Goyer, John (2020) 'US Must Recapture Lost Ground in Southeast Asia or Risk Being Shut Out'. The Diplomat, https://thediplomat.com/2020/02/us-must-recapture-lost-ground-in-southeast-asia-or-risk-being-shut-out/

[179] Tang, S.M. et al. (2020) 'The state of Southeast Asia: 2020'. ISEAS-Yusof Ishak Institute https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf

[180] Bendett, Samuel & Kania, Elisa (2019) 'A new Sino-Russian high-tech partnership'. Australian Strategic Policy Institute. https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership

[181] ASEAN-2019 Business and Investment Summit. https://tass.com/economy/1086743

[182] Association of Southeast Asian Nations (ASEAN) (2018) 'Statement of ASEAN and the Russian Federation on Cooperation in the Field of Security of and in the Use of Information and Communication Technologies'. https://asean.org/storage/2018/11/FINAL-Statement-of-ASEAN-and-the-Russian-Federation-on-Cooperation-in-the-Field-of-Security-of-and-in-the-Use-of-Information-and-Communication-Technologies.pdf

[183] Association of Southeast Asian Nations (ASEAN) (2018) 'Statement of ASEAN and the Russian Federation on Cooperation in the Field of Security of and in the Use of Information and Communication Technologies'. https://asean.org/storage/2018/11/FINAL-Statement-of-ASEAN-and-the-Russian-Federation-on-Cooperation-in-the-Field-of-Security-of-and-in-the-Use-of-Information-and-Communication-Technologies.pdf

[184] Association of Southeast Asian States (2020) 'The 18th ASEAN–Russia Joint Cooperation Committee Meeting'. https://asean.org/18th-asean-russia-joint-cooperation-committee-meeting/

international community.[185] Korea focuses in its cooperative actions with ASEAN on innovation, connectivity enhancement, human resource development and information security. These actions are also highlighted in the ASEAN–Korea 2019 ICT work plan.[186] Korea also supports interregional cooperation with the EU and the OSCE.[187]

Australia is positioning itself as a strong international cybersecurity actor with its international cyber engagement strategy. Following the strategy, Australia champions an open, free and secure cyberspace by building capacity in cybercrime capabilities, developing national cybersecurity practices, advocating for multi-stakeholder governance and fostering dialogue on the application of international law and the implementation of norms in cyberspace, with a primary regional focus on the Indo-Pacific.

Australia's Cyber Cooperation Program, for which it partnered with many ASEAN member states and non-state actors, works across the Indo-Pacific to improve cyber resilience.[188] They created the ASEAN–Australia Digital Trade Standards Cooperation initiative to improve digital economy and streamline trade.[189] The Jakarta Centre for Law Enforcement Cooperation in Indonesia, which provides training to combat cybercrime, is a bilateral undertaking with Australia. ASEAN and Australia have been actively working on capacity building with INTERPOL in the region, and promoting the Budapest Convention.[190]

While a strong ally of the US, Australia is also adopting ASEAN's centrality approach, stating that it won't take sides in terms of who it cooperates with. This shows Australia's vulnerability to unchecked rivalry between the US (its most important strategic ally) and China (its largest trading partner).[191]

[185] Information Security Policy Council Japan (2018) 'Summary of the [sic] Japan's Cybersecurity Strategy'. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf

[186] Both Japan and Korea have a separate engagement roadmap created by the EUCyber Direct project, focusing more on their national and international cybersecurity progress.

[187] Organization for Security and Cooperation in Europe (OSCE) (2015) 'The OSCE Asian Partnership for Co-operation: Reflections and Perspectives'.https://www.osce.org/partners-for-cooperation/asian/197801

[188] Ongoing developments of Australia's Cyber Cooperation Program can be found at https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/cyber-cooperation-program

[189] Progress on the Australian standardisation initiative on digital trade with ASEAN is available at https://www.standards.org.au/engagement-events/international/asean-australia-digital-trade

[190] INTERPOL, 'ASEAN Cyber Capacity Development', last accessed 18/03/2021. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-training-for-police/ASEAN-Cyber-Capacity-Development

[191] Stromseth, Jonathan (2019) 'Don't make us choose: Southeast Asia in the throes of US-China rivalry'. Brookings Institute. https://www.brookings.edu/research/dont-make-us-choose-southeast-asia-in-the-throes-of-us-china-rivalry/

6 The EU and South-East Asia

In a 2020 survey of ASEAN experts and policy influencers by the Singaporean ISEAS-Yusof Ishak institute, the EU was deemed the best actor for maintaining the rule-based order and upholding international law, and the second most preferred and trusted strategic power for the region, after Japan and before the US and China. The biggest reason for this trust, according to respondents, was that they found the EU to be a responsible stakeholder that respects and champions international law.[192]

Apart from the EU's common interests in strengthening the rules-based international order and in effective multilateralism, the EU's priorities in the Asia-Pacific and specifically the South-East-Asian region have a major economic aspect. The EU has become the second largest trading partner for ASEAN, and ASEAN is the third largest trading partner for Europe. The EU is the largest source for foreign investment, and has also provided the most development assistance for the ASEAN secretariat and regional integration.[193]

6.1 Policies

The EU's relationship with ASEAN was elevated in 2020 to an EU–ASEAN Strategic Partnership. This committed the partners to regular summits at leaders' level and established the importance of the relationship.[194]

The EU managed to describe a common approach on peace and stability in cyberspace in these Council Conclusions, thereby crystallising cybersecurity as a priority for all of Asia.

The EU regards support to ASEAN's inclusive multilateral architecture in the region as an important objective, as it was described as a main priority in the ASEAN–EU plan of action 2018–2022.[195] The same plan of action described how the two regions are committed to cooperate on conflict management and peacebuilding initiatives in the region, as the EU sees ASEAN as a peaceful influencer in the region.[196] This commitment to security was first formalised in 2012, when the EU became the first regional organisation to accede to the Treaty of Amity and Cooperation in Southeast Asia (TAC), a non-aggression and cooperation pact.[197] The EU's commitment to security was repeated in the 2018 Council Conclusions on enhanced EU security cooperation in and with Asia. The EU managed to describe a common approach on peace and stability in cyberspace in these Council Conclusions, thereby crystallising cybersecurity as a priority for all of Asia.[198]

[192] Tang, S.M. et al. (2020) 'The State of Southeast Asia: 2020.' ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf

[193] Association of Southeast Asian Nations (ASEAN) (2020) 'Joint Press Statement – 27th ASEAN–EU Joint Cooperation Committee (JCC) Meeting Convenes in Jakarta'. https://asean.org/joint-press-statement-27th-asean-eu-joint-cooperation-committee-jcc-meeting-convenes-jakarta/

[194] European External Action Service (2020) "EU-ASEAN Strategic Partnership Factcheck" https://eeas.europa.eu/sites/default/files/fact-sheet-eu-asean-strategic-partnership.pdf

[195] Association of Southeast Asian Nations (ASEAN) (2018) '1st ASEAN Regional Forum Inter-sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF ISM on ICTs Security)' Co-Chairs' Summary Report'. http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-12.pdf

[196] European External Action Service (EEAS) (2017) 'ASEAN–EU Plan of Action 2018–2022'.

[197] European Council (2012) 'Treaty of Amity and Cooperation in Southeast Asia'. *Official Journal of the European Union*, Council Decision 2012/308/CFSP. http://ec.europa.eu/world/agreements/downloadFile.do?fullText=yes&treatyTransId=14961

[198] Council of the European Union (2018) 'Enhanced EU Security Cooperation in and with Asia – Council Conclusions'. 9265/1/18. https://www.consilium.europa.eu/media/35456/st09265-re01-en18.pdf

In a 2019 joint statement on cybersecurity cooperation, the EU and ASEAN committed to contribute to the advancement of an open, secure, stable, accessible and peaceful ICT environment.[199] While this is a notable effort, the EU is challenged with cultural differences in the exact interpretations of these terms. In this 2019 joint statement, the EU committed itself to further engagement through relevant ASEAN-led mechanisms such as the ARF's ISM on ICT security, TELMIN and the AMCC to foster common understanding. The EU is a founding member of the ARF, where it directly participates in the ASEAN central security architecture. In the ARF's ISM on ICT security, the EU is an active participant on implementing CBMs. The EU is the co-lead with Singapore on CBM#3 on protection of critical infrastructures and consultation mechanisms.[200]

The EU Commission's DG Connect has a yearly exchange with TELMIN to discuss digital economy and connectivity issues, exchange best practices on developing a digital single market, and advance EU–ASEAN digital cooperation.[201] In 2019 they developed an ASEAN–EU ICT workplan, to improve cybersecurity capacities. It prioritises the creation of an ASEAN digital economy and society benchmarking index.[202]

6.2 Initiatives

The EU has several initiatives and instruments with ASEAN to put its commitments to a rules- and rights-based stable cyberspace into practice. The regional **EU–ASEAN dialogue instrument** (E-READI) is the main funding instrument for cooperation between the regions, and also funds several activities in the ICT sector. The **ASEAN–EU ICT workplan** built with the European Commission's DG Connect will be implemented with this instrument.[203]

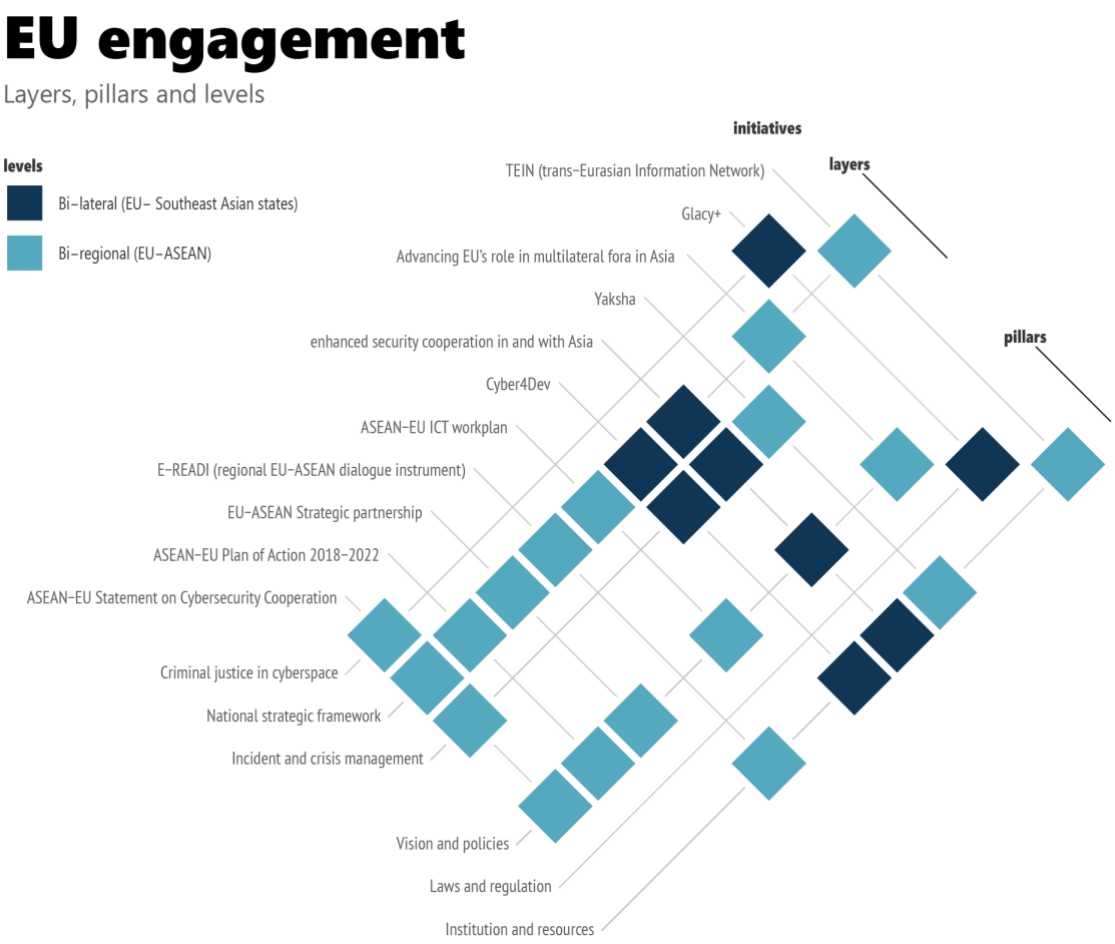
[199] European External Action Service (2019) 'ASEAN–EU Statement on Cybersecurity Cooperation'. https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf

[200] ASEAN Regional Forum (ARF) (2019) 'Co-Chairs' Summary Report of the 2nd ARF ISM on ICTs Security Singapore', 28–29 March 2019.

[201] The EU and ASEAN: Building Stronger Digital Economy & Connectivity Cooperation. https://digital-strategy.ec.europa.eu/en/library/eu-and-asean-building-stronger-digital-economy-connectivity-cooperation

[202] Association of Southeast Asian States (2019) 'Joint Media Statement of the 19th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings'. https://asean.org/storage/2019/10/ADOPTED-TELMIN-19th-TELMIN-JMS-.pdf

[203] European External Action Service (2018) 'EU-ASEAN leaders held high level meeting to enhance cooperation', European Union Mission to ASEAN, https://eeas.europa.eu/delegations/association-southeast-asian-nations-asean/52443/eu-asean-leaders-held-high-level-meeting-enhance-cooperation_en



The European Commission Directorate General on International Partnerships (formerly DEVCO) has been focusing on building digital capacities. Its recent **Digital for Development (D4D)** guidelines, created in 2017, mainstream digital technologies and services into the EU's development policy and initiatives already present in the region.[204] With **Cyber4Dev**, the European Commission funds the building of cyber resilience capabilities in three ASEAN countries: Cambodia, Indonesia and Laos. This project is delivered by Northern Ireland Cooperation Overseas in partnership with government agencies from Estonia, the United Kingdom and the Netherlands, and works with local expertise and stakeholders on building policies and training for cyber incidents.[205]

Cyber4Dev is funded through the Foreign Policy Instrument Contributing to Stability and Peace (IcsP), together with the Global Action on Cybercrime (GLACY) and its successor **GLACY+ project**. This is implemented by the Council of Europe and is active in Vietnam, Thailand, Timor Leste, Singapore, the Philippines, Myanmar, Malaysia and Indonesia. GLACY+ helps these countries strengthen their law enforcement capabilities to battle cybercrime and implement domestic legislation and policies related to cybercrime and cybersecurity, while respecting human rights and rule of law standards. It also helps them to improve their abilities for effective international cooperation on cybercrime, in particular in line with the Budapest Convention. [206] The Philippines is a priority and hub country for capacity building

[204] European Commission Staff Working Document (2017) 'Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy'. https://ec.europa.eu/international-partnerships/system/files/swd-digital4development-part1-v3_en.pdf

[205] Cyber4Dev project activities (last consulted 21 March 2021) https://cyber4dev.eu/project-activities/

[206] Council of Europe (2020) 'Global Action on Cybercrime Extended (GLACY+) Project Summary'. https://rm.coe.int/3148-glacy-summary-v5/16809c8ad6

under the GLACY+ project as it is the only country in the region that has acceded to the Budapest Convention, in March 2018.

To complement existing dialogues and efforts, the EU launched an initiative to enhance **security cooperation in and with Asia** through partner countries Indonesia, Vietnam, Japan, Republic of Korea and India. It addresses four shared security challenges, including cybersecurity through peer-to-peer cooperation, exercises and training, and Track 1.5 and Track 2.0 dialogues. This multi-donor action is co-financed by the EU, the German Federal Foreign Office and the French Ministry for Europe and Foreign Affairs. It is implemented by GIZ and Expertise France.[207] The European project on **advancing the EU's role in Multilateral Fora in Asia** also strengthens the EEAS engagement with both ASEAN as the wider Asian region through the ARF and the Asia–Europe Meeting (ASEM). The project offers its support to organise and communicate events relating to security issues of which cybersecurity is seen as a non-traditional security issue.[208]

The **Trans-Eurasian Information Network (TEIN)** has been connecting research networks in the Asia-Pacific to the European GEANT network and researchers since 2001, and has greatly improved digital interconnectivity. It is currently working on bridging the digital divide in the region, providing an alternative to Chinese investments.[209]

With the Horizon 2020 project **YAKSHA**, the EU is also developing and implementing a software toolkit to improve cybersecurity of organisations in the ASEAN region.[210] The EU was mentioned as a partner with which the new ASEAN–Singapore Cyber Centre of Excellence and the ASEAN–Japan Cybersecurity Capacity Building Centre in Thailand would design and deliver cybersecurity capacity building programmes.[211] The establishment of the centres is a great opportunity to engage with the regional stakeholders and work on capacity building on the region's terms and in line with Asian values.

The EU has mostly held diplomatic engagement with ASEAN member states through regional cooperation. There has not been much bilateral cooperation with South-East Asia. This has been more successful for non-ASEAN countries. The EU currently has digital dialogues with Japan, Korea, India and China, which also play an important role in South-East Asia.[212]

[207] European Commission (2019) 'Security Cooperation in and with Asia: Action Document Annex 3' https://ec.europa.eu/fpi/sites/fpi/files/annexe_3_security_cooperation_in_and_with_asia_part1_v2.pdf

[208] Project Description 'Advancing European Union's role in Multilateral Fora in Asia'. https://eu-cyber-direct.s3.eu-central-1.amazonaws.com/eu-cyber-direct/assets/gzFWzG46/advancing-eu-role-in-multilateral-fora-in-asia-brochure.pdf

[209] European Commission 'Asia – The Trans-Eurasia Information Network (TEIN)'. https://ec.europa.eu/europeaid/regions/asia/tein-3_en

[210] EU DG CONNECT (2018) 'Project YAKSHA to reinforce EU-ASEAN cooperation in cybersecurity'.

[211] Cyber Security Agency Singapore (2019) 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019'. https://www.csa.gov.sg/news/speeches/asean-ministerial-conference-on-cybersecurity-2019

[212] More information on EU engagement with these countries is extensively discussed in the EU Cyber Direct Dialogue papers on these countries, available at www.eucyberdirect.eu

7 Conclusions

Insights into ASEAN cohesion and how ASEAN is positioned in the world provide better understanding of how the EU can engage with this region, and leverage support for stability in cyberspace. In terms of ASEAN cohesion, it became clear that initiatives will not thrive in the diverse South-East Asian region as long as there is no consensus over principles. Developments discussed in this paper show that there is now consensus on cybersecurity cooperation, in both 'how' and 'what'. The 'ASEAN way' has provided a good guiding principle on how ASEAN member states would cooperate on cybersecurity. The emphasis on sovereignty creates a unique type of cybersecurity cooperation in the world. It leaves much room for national responsibility in cybersecurity development, which respects the different levels of maturity in the region, yet it aims to create collective resilience against cyberthreats.

Whether states will be incentivised to improve their due diligence without binding instruments is uncertain, but countries in the region have shown commitment by actively participating in the ministerial conferences on cybersecurity. South-East Asian cooperation is centred on capacity-building initiatives. This started with the ASEAN capacity building programme and led to the creation of the ASEAN–Singapore Cybersecurity Centre of Excellence and the ASEAN–Japan Cybersecurity Capacity Building Centre. These intend to increase the maturity of all ASEAN countries.

To understand what exactly ASEAN member states are cooperating on, it is useful to know that there appear to be three types of country in ASEAN: those that are technologically advanced and have invested in cybersecurity; those that have developed their digital infrastructure but have not reached cybersecurity maturity; and those that have a low level of digital connectivity.[213] For these last countries, the priority is not on cybersecurity maturity or even critical infrastructure, but mostly on getting them to the same level of digital maturity. Regardless of a lack of advanced infrastructure that would be vulnerable to cyberattacks, ASEAN cooperation on cybersecurity will limit itself to issues that have a technology focus. All ASEAN states are treating the issues that arise with online interactions (disinformation, critique of governments, terrorism, etc.) as domestic issues, preventing them from becoming part of cybersecurity cooperation. Such an approach allows a discussion on cyber norms among themselves and with partners like the EU where ideological disagreements on content-related aspects of internet governance can be avoided.

The willingness of South-East Asian governments to work with relevant stakeholders is an interesting development, as ASEAN states recognised the shared responsibility of the wide variety of actors. Partnerships with the technical community, private sector and civil society are on the horizon, even if these actors have not been deeply involved in discussions on norms of state behaviour in cyberspace. Civil society in particular seems to be lacking in countries that are grappling with the challenges of the increasing digital penetration in society, with the exception of some encouraging new initiatives. Those countries' participation is essential to develop cybersecurity policies that respect human rights.

ASEAN states agreed with the EU in 2019 that they support a rule-based internet; believe in shared responsibility for governing the internet; and will commit to open, secure, stable, accessible and peaceful ICTs.[214] South-East Asia is however in a different geopolitical position than Europe, which is crucial to understand in any diplomatic venture. The region is always doing a balancing act, clinging to its rights to sovereignty. Voting behaviour of South-East Asian states in international fora has reflected this balancing exercise, brokering between proposals that reflect a state-centric view of cybersecurity governance and a market-based multi-stakeholder view on cyberspace, which they do not see as

[213] Raska, Michael & Ang, Benjamin (2018) 'Cybersecurity in Southeast Asia'. Introductory note to the roundtable on 22 May 2018, Southeast Asia Observatory https://centreasia.eu/en/cybersecurity-in-southeast-asia-benjamin-ang-dr-michael-raska-2/

[214] European External Action Service (2019) 'ASEAN–EU Statement on Cybersecurity Cooperation'. https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf

necessarily contradictory. The EU's partnerships with like-minded states in the region is crucial to support South-East Asia's balancing act.

How ASEAN states themselves perceive norms of responsible state behaviour in cyberspace is gradually becoming more apparent, though it will be imperative to develop answers to tricky questions such as how they perceive the application of international law in the case of incidents. A commendable effort to exchange perspectives is being undertaken at the ASEAN Regional Forum, of which the EU is also a member. The development of CBMs can increase transparency between competing actors in the region, such as China, Russia and the US.

All in all, the high trust between the EU and ASEAN and their shared goals foster a stable partnership to work together on creating a rights- and rules-based cyberspace.

About the author

Nathalie Van Raemdonck is a doctoral researcher at the Vrije Universiteit Brussels where she focuses on platform governance, the organic spread of misinformation and online radicalization. Prior to joining academia, she was an Associate Analyst at the EU Institute for Security Studies and worked at the Centre for Cybersecurity Belgium and the Cyber Emergency Response Team. Follow her on Twitter @eilah_tan

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

DIGITAL DIALOGUES

are a series of research papers providing an overview of selected issues, policies and institutions of the EU's main strategic partners.

EU CYBER DIRECT

This project is funded by the European Union.