The Commonwealth

Commonwealth Cybercrime Journal \ 133
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Cyber Diplomacy Co-operation on Cybercrime between Southeast Asia and Commonwealth Countries: Realities, Responses and Recommendations

Mark Bryan Manantan[1]

Abstract

Amid the onslaught of the COVID-19 pandemic, Southeast Asia's technological innovation footprint has expanded, and its digital economy continues to mature. However, Southeast Asia's vulnerability to cyber threats like cybercrime is also accelerating at a pace commensurate with the region's digital transformation. As geopolitical powerplay colours regional and international co-operation on cybercrime, Southeast Asia's digital prospects will rely on new ways of collaboration. This article examines the growing security implications of cybercrime in Southeast Asia, aiming to formulate effective policy interventions to advance regional and international cyber diplomacy co-operation – through capacity building and multistakeholder partnerships – against the backdrop of the Association of Southeast Asian Nations' (ASEAN's) declining political and institutional power, worsening geostrategic rivalry, and the stalemate of international co-operation on internet governance. It advances the concept of peer-to-peer learning as a practical yet flexible approach to drive cyber diplomacy engagements that will bring key stakeholders together across different jurisdictions. This approach could potentially jumpstart pan-ASEAN co-operation in the short-to-medium term, given the lack or absence of a regional framework on cybercrime.

1 Director, Cybersecurity and Critical Technologies, Pacific Forum.

The article further explores the peer-to-peer learning model to facilitate cross-regional co-operation among Southeast Asia and Commonwealth countries in Africa, Latin America and the Pacific Island nations. By leveraging a strong network and expertise of law enforcement agencies, regulatory bodies, financial institutions, technology ('tech') companies and civil society organisations located in various jurisdictions through regular exchanges, it becomes plausible to analyse the full scale of cybercrime threats and consequently manage their risks. In effect, developing economies can then prioritise and manage resources effectively to enhance cross-regional cybercrime collaboration, despite the current fragmentation of global internet governance.

Introduction

The COVID-19 pandemic has catalysed Southeast Asia's rapid digital transformation. Since the pandemic, 60 million Southeast Asians have gone online – prompting users to use digital platforms to cope with the disruptions of intermittent lockdowns and the rapid shift to remote working. That meant increased dependence on mobile and cloud services, as well as e-commerce and distance learning.[2] As Southeast Asia eases into the 'new normal', digital adoption is not slowing down. If the trend persists, the region's digital economy could reach approximately US$1 trillion in gross merchandise value by 2030.[3]

Southeast's Asia's prospects in the global digital economy are largely premised on its increasing importance as an emerging online market and its potential to drive innovation through its homegrown tech companies.[4] With more than 887 mobile connections comprising 132 per cent of its total population in 2021, the region is leading in the adoption of mobile connections.[5] With over 400 million users plugged into the internet, digital services such as e-commerce, online media, online banking and finance, health tech, and education tech ('edtech') are expected to continue to thrive.[6] Such a bullish outlook has propped up the region as a lucrative destination of capital investments, recording a deal value of US$11.5 billion in the first half of 2021 alone – one that exceeded

2 Manantan, MB (2022), 'US-Singapore: Advancing Technological Collaboration and Innovation in Southeast Asia', *Issues and Insights,* Vol. 22 No. 5, September, available at: https://pacforum.org/publication/issues-insights-vol-22-sr5-us-singapore-advancing-technological-collaboration-and-innovation-in-southeast-asia.

3 Bain & Company (2021), 'e-Conomy SEA Report 2021: Southeast Asia enters its "digital decade" as the internet economy is expected to reach US$1 trillion in Gross Merchandise Value (GMV) by 2030', 10 November, available at: https://www.bain.com/about/media-center/press-releases/2021/sea-economy-report-2021/.

4 Manantan, MB (2022), 'US-Singapore: Advancing Technological Collaboration and Innovation in Southeast Asia'.

5 Neo, K (2021), 'Digital 2021 Southeast Asia Regional Overview', *We are Social*, 8 March, available at: https://wearesocial.com/sg/blog/2021/03/southeast-asia-digital-life-intensified/

6 Bain & Company (2021),'e-Conomy SEA Report 2021', op. cit. note 3.

2020's cumulative inflow of US$11.6 billion.[7] The increased deal activity and larger valuations have prompted tech companies, especially start-ups, to explore Initial Public Offerings (IPOs) to further raise capital and/or entice investors to monetise their holdings.

The Association of Southeast Asian Nations (ASEAN), a regional bloc comprising ten member states – Indonesia, Malaysia, Singapore, the Philippines, Thailand, Vietnam, Brunei, Cambodia, Myanmar, and Laos – has laid out the foundation of the region's digital economic aspirations under the ASEAN Economic Community blueprint released in 2015.[8] Recognising the unprecedented changes brought by the pandemic, and the urgency of jumpstarting economic recovery, ASEAN published an updated version of its Digital Master Plan 2025. Additionally, the release of the Brunei-led Bandar Seri Begawan Roadmap further cements ASEAN's desire to leverage technology and digital trade to spur economic recovery over the medium-to-longer term.[9]

At the individual country levels, Indonesia, Malaysia, Singapore, Thailand, and Vietnam have released their respective national policy and strategy documents and even roadmaps outlining their vision to seize the opportunities of the emerging data-driven economy. Amid their varying rollout of fifth-generation technology ('5G') and adoption of emerging technologies like artificial intelligence (AI), the region is unequivocally upbeat about riding the momentum of digital transformation.[10] Therefore, the answer to whether the region can withstand the headwinds of its digital transformation journey – due to digital skills shortages and uneven digital infrastructure – is that it will have to.

However, equally concerning to the digital structural challenges that have beset Southeast Asia are the risks and vulnerabilities brought by the rapid digital transformation. As more public and private organisations become interconnected to the 5G network, they are increasingly employing AI-enabled technologies and internet of things (IoT), while migrating to the cloud platform. This integration of digital technologies has expanded the attack surface that malicious cyber actors can exploit. During the pandemic, Naikon – and advanced persistent threat (APT) group – targeted several governments in the Philippines, Vietnam, Thailand, Myanmar and Brunei to gather geopolitical intelligence.[11] Similarly, SharpPanda – a Chinese-linked APT group – also used sophisticated spear phishing emails, a malicious tactic which targets very specific individuals and organizations to obtain classified information. In addition, nefarious actors also installed backdoors to conduct surveillance operations against Southeast Asian governments. Extant cybersecurity

7 Ibid.
8 The Internet Society and TRPC Ltd. (2015),'Unleashing the Potential of the Internet for ASEAN Economies', available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC_ASEAN_Digital_Economy_Report_Full_s.pdf.
9 Manantan, MB (2022) 'US-Singapore', op. cit. note 2.
10 Noor, E and MB Manantan (2022), 'Raising Standards: Data and Artificial Intelligence in Southeast Asia,' *Asia Society Policy Institute*, July, available at: https://asiasociety.org/sites/default/files/inline-files/ASPI_RaisingStandards_report_fin_web_0.pdf.
11 *Checkpoint* (2020), 'Naikon APT: Cyber Espionage Reloaded,' *Checkpoint*, 7 May, available at: https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

literature on Southeast Asia has focused mainly on the strategic implications of state-sponsored APT groups centred on geopolitical flashpoints like the South China Sea.[12] However, the consequential implications of the lack of a regional approach to cybercrime remains underexplored in Southeast Asia. The urgency of adopting more concrete steps that go beyond strengthening cyber hygiene or cyber awareness has received underwhelming attention.[13] This article seeks to fill that gap.

In recent years, cybercrimes that span the spread of malware, ransomware, distributed denial of service attacks (DDoS), data breaches and phishing have seen a dramatic surge in Southeast Asia. Due to increased connectivity, exacerbated by the uncertainty of pandemic lockdowns, cybercriminals have exploited the brewing social anxieties to access, steal and profit from stolen data.[14] With more than 50 per cent of companies based in Singapore falling prey to ransomware in 2021, Singapore's Cybersecurity Agency elevated cybercrime as a legitimate national security risk due to its capacity to cripple networks of large enterprises and, more importantly, compromise the daily operations of small and medium-sized businesses.[15] Despite the obvious threats that cybercriminals pose, ASEAN still needs to adopt a regionwide approach against cybercrime that would facilitate deeper regional co-ordination among law enforcement agencies. The regional bloc's growing list of geopolitical concerns – the South China Sea[16] and Myanmar coup,[17] among others – and the looming pressure to restart the post-pandemic economic recovery are putting major stress on its capacity to demonstrate political and institutional authority. Furthermore, multilateral discussions on a cybercrime treaty have also stalled due to the geopolitical powerplay between the US and China.

12 Manantan, MB (2020), 'The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea', *Issues & Studies*, Vol. 56 No. 3, available at: https://www.worldscientific.com/doi/10.1142/S1013251120400135; Gomez, MA (2013), 'Awaken the Cyber Dragon: China's Cyber Strategy and Its Impact on ASEAN', *Journal of Communication and Computer,* Vol. 10, available at: https://www.academia.edu/3082490/Awaken_The_Cyber_Dragon_Chinas_Cyber_Strategy_and_Its_Impact_on_ASEAN.

13 Chang, LYC (2020), 'Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia', *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 6 June, available at: https://link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3_6.

14 UN Office on Drugs and Crime (UNODC) (2021),'Cybercrime and COVID19 in Southeast Asia: an evolving picture', available at: https://www.unodc.org/documents/Advocacy-Section/UNODC_CYBERCRIME_AND_COVID19_in_Southeast_Asia_-_April_2021_-_UNCLASSIFIED_FINAL_V2.1_16-05-2021_DISSEMINATED.pdf

15 Low, D (2022), 'Ransomware attacks threaten nations, 137 S'pore firms fell prey in 2021: CSA', *The Straits Times*, 29 August, available at: https://www.straitstimes.com/tech/tech-news/ransomware-attacks-threaten-nations-137-spore-firms-fell-prey-in-2021-csa.

16 Manantan, M (2019), 'The Cyber Dimension of the South China Sea Clashes', *The Diplomat*, 5 August 2019, available at: https://www.philstar.com/headlines/2022/12/21/2232369/philippines-concerned-over-report-chinas-construction-activities-spratlys

17 Editorial Board ANU (2023), 'Myanmar presents ASEAN with only bad options', *East Asia Forum*, 16 January 2023, available at https://www.eastasiaforum.org/2023/01/16/myanmar-presents-asean-with-only-bad-options/

This article will examine the growing security implications of cybercrime in Southeast Asia in order to suggest effective policy interventions to advance regional and international cyber diplomacy co-operation against the backdrop of ASEAN's declining political and institutional power, worsening geostrategic rivalry, and the stalemate of co-operation on internet governance at the global level. Defined as the use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace – mainly through the provision of cyber capacity-building and confidence-building measures, and the development of norms – 'cyber diplomacy' allows the exchange of technical and policy know-how to build resilience against cybercrime.[18] Although Southeast Asia has become an active player in cyber diplomacy itself, the disruptive nature of emerging technologies and the shifting modus operandi of state-sponsored hackers and cybercrime groups have left the region scrambling for effective and agile solutions.

Given the situation, this article seeks to explore other avenues that defy the conventional dyad of co-operation between ASEAN and its existing dialogue partners like the US, Japan, Australia, China, South Korea etc. The article argues that countries in Southeast Asia could adopt a peer-to-peer learning approach to cyber diplomacy engagements beyond the 'usual suspects'. This means engaging other key stakeholders from various sectors across different jurisdictions, such as those located in Africa, Latin America, or Pacific Island nations. The proposed peer-to-peer learning approach could potentially catalyse fresh and innovative analysis to fortify regional co-operation against the risks and vulnerabilities of cybercrime in the short-to-medium term.

This article defines a peer-to-peer learning approach based on a collaborative partnership that involves developing economies, mainly via Global South-to-South dynamics, and goes beyond the conventional developed–developing country relationships.[19] Through the adoption of peer-to-peer learning among the technologically advanced countries in Southeast Asia – comprising of Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam – the article will offer key insights that can strengthen ASEAN's declining decision-making processes in the face of urgent and rising threats like cybercrime. In exploring the peer-to-peer learning approach, the article aims to further enrich the cyber diplomacy literature, specifically the cyber capacity-building portfolio in Southeast Asia that has often been dominated by literature on donor–recipient relations, primarily from ASEAN's dialogue partners like Japan and Australia.[20] The article also contends that the peer-to-peer learning model could help facilitate deeper co-operation among Southeast Asia and Commonwealth countries in Africa, Latin America and the Pacific Island nations. With shared interests towards maintaining an inclusive, neutral and multilateral

18 Manantan, MBF (2021), 'Advancing cyber diplomacy in the Asia Pacific: Japan and Australia', *Australian Journal of International Affairs*, available at: https://www.tandfonline.com/doi/full/10.1080/10357718.2021.1926423.

19 Collett, R (2021), 'Understanding cybersecurity capacity building and its relationship to norms and confidence-building measures', *Journal of Cyber Policy* , available at: https://www-tandfonline-com.ezproxy.lib.rmit.edu.au/doi/full/10.1080/23738871.2021.1948582?src=recsys.

20 Manantan, MBF (2021) 'Advancing cyber diplomacy in the Asia Pacific', op. cit. note 15.

platform, small and medium power countries can bond together to co-ordinate on a narrow and well-defined set of functional areas of co-operation, such as cybercrime, that demonstrate their agency and autonomy. Due to the intense competition brought by the US and China, the concept of peer-to-peer learning serves as an attractive and viable model for a co-operative framework. It could jumpstart cross-regional co-operation among countries in Southeast Asia, South Asia, Africa, Latin America and the Pacific amid the uncertainty of achieving international consensus on cybercrime co-operation in the foreseeable future.

The article expands on its main argument in three stages. First, it will conduct a brief examination on the underlying *realities* of technologically capable countries in Southeast Asia against the growing threats of cybercrime. From there, it will examine the *responses* undertaken at the regional level through ASEAN and at the individual country level. This section will highlight various avenues through which Southeast Asia is 'bridging the gap' in terms of internal and external capacity-building co-operative mechanisms. After this assessment, the paper will offer policy *recommendations* on how Southeast Asia can play a more proactive role in cyber diplomacy in tackling cybercrime through peer-to-peer learning within the region, as well as exploring collaboration with Commonwealth countries in Africa, Latin America and the Pacific Islands nations.

Realities: setting the cybercrime landscape

Due to increasing digital connectivity and compounded by the social anxieties from the pandemic, Southeast Asia has become a fertile ground for cybercriminals to test and launch their illicit activities. More importantly, the region's weak and/or absent legislative and policy frameworks for investigating and prosecuting cyber-related crimes make it the ideal operational environment for cybercriminals and syndicates to conduct and continuously refine their operations. This section provides an overview of the cybercrime landscape in Southeast Asia, highlighting (1) prevailing cybersecurity threats, trends and tactics employed by malicious actors; (2) rising incidents of ransomware and exploitation of cryptocurrency; and (3) an absence of cybercrime policies and legislative gaps.

Prevailing cybersecurity threats, trends, and tactics

The Asia Pacific region, particularly Southeast Asia, has higher-than-average rates of malware and ransomware attacks. Microsoft found that the region has rates 1.6 or 1.7 times higher than the global average.[21] Through a concerted and collaborative partnership with key stakeholders from the public and the private sectors, Interpol's *ASEAN Cyberthreat Assessment 2021* report identified the following as the top cybercrime threats: (1) business e-mail compromise (BEC); (2) phishing; (3) ransomware;

21 Microsoft Stories Asia (2022), 'Microsoft launches first Asia Pacific Public Sector Cyber Security Executive Council across seven markets in the region', 31 May, available at: https://news.microsoft.com/apac/2021/05/31/microsoft-launches-first-asia-pacific-public-sector-cyber-security-executive-council-across-seven-markets-in-the-region/.

(4) e-commerce data interception; (5) crimeware-as-a-service; and (6) cyber fraud. Interpol ranked ransomware as the most significant threat in Southeast Asia, one that is proliferating at an unprecedented rate because barriers to entry are low, and it is affordable to execute. In addition, ransomware-as-a-service (RaaS), crimeware-as-a-service (CaaS) and phishing-as-a-service (PhaaS) are also becoming popular for making a quick profit. These are business models between ransomware operators and affiliates. In this set-up, affiliates, who do not have the skillset to develop ransomware, pay operators to launch ransomware attacks. Put simply, RaaS, CaaS, and PhaaS operate in a similar fashion to the software as a service (SaaS) business model.[22] Interpol also emphasised the increasing propensity among cybercriminals to exploit the growing ubiquity of IoT devices, using various tactics to obtain maximum illicit gains. The report also noted that open-source information is vital to crafting effective social engineering scam tactics against individuals and organisations.[23] Furthermore, with the e-commerce boom, cybercriminals are deploying an increasing number of JavaScript card sniffers to siphon proprietary financial and personal information.

Rise in ransomware incidents and exploitation of cryptocurrency

Microsoft's Digital Crimes Unit made parallel observations, noting the low-cost yet high-profit yield of ransomware as a cybercriminal activity. Meanwhile, well-resourced cybercriminals who can operate at larger scales have deployed armies of infected computers to launch simultaneous malware attacks. Other cybercriminals have adopted a 'mix and match strategy'; for instance, BEC have used sophisticated phishing attacks to lure victims, steal information and redirect money to criminal bank accounts, while tech-support scams have been quite effective, especially amid the looming financial distress that took place at the height of the COVID-19 pandemic.[24]

Based on a survey of more than 900 IT executives and professionals, Kaspersky found that 67 per cent of businesses in Southeast Asia had become victims of cybercrime in 2020. Most of the victims (82.1%) confessed to having paid the ransom demand – higher than the global average of 38.1 per cent.[25] Kaspersky also reported that 47.8 per cent of the victims paid the ransom as soon as possible to mitigate any disruption to business operations, while 23.9 per cent attempted to recover data through backup or decryption before giving in and having to pay within two days. Only a small percentage, 10.4 per cent,

22 Baker, K, 'Ransomware as a Service (RAAS) Explained How It Works & Examples', *Crowdstrike*, January 30, 2023, available at https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

23 Interpol (2021), *ASEAN Cyberthreat Assessment 2021*, available at: https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf.

24 Manantan, MB and D Mitchum (2021), 'Key Findings Adapting to COVID-19 Indonesia, the United States, and the Indo-Pacific', Session #2 Assessing Cybersecurity Trends and Threats in the US and Indonesia, Pacific Forum, 29 March, available at: https://pacforum.org/wp-content/uploads/2021/03/210329_US-Indonesia_KeyFindings.pdf.

25 Zulhusni, M (2022), '67% of businesses in SEA found themselves as victims of ransomware attacks', *Techwire Asia*, 17 August, available at: https://techwireasia.com/2022/08/67-of-businesses-in-sea-found-themselves-as-victims-of-ransomware-attacks/.

resisted for a week and eventually paid the demand ransom. According to the *Unit 42 Ransomware Threat Report 2021*, the average ransom demand has increased up to 144 per cent, citing an 85 per cent surge in the number of victims whose names and details were posted on the dark web's leak sites. The hack and leak modus operandi of cybercriminals is proving to be one of the most evolving coercive tactics among cybercriminal groups, the aim being to increase the pressure on their victims with the ultimate end goal of demanding a higher ransom.[26]

Conducting a deeper analysis on the increasing role of the dark net in facilitating cybercrime in the region, the United Nations Office on Drugs and Crime (UNODC) confirmed the alarming rise in dark net cybercrime in Southeast Asia.[27] The dark web has become a major platform for people to engage in illicit activities, from buying and selling cybercrime toolkits, acquiring stolen credit card details and personal identifiable information from breaches, to trading online child sexual exploitation material.[28] Cryptocurrencies are the primary payment method on dark nets, while Bitcoin is the primary tool to exchange crypto to fiat (that is, the currency issued by countries).

Southeast Asia's proximity to key cyber actors like North Korea make it both a target and an accomplice in cybercrime. In 2019, the UN Security Council's Sanctions Committee on North Korea revealed how Pyongyang's cyber activities stole billions of dollars from financial institutions and cryptocurrency exchanges to generate income.[29] Lazarus, a North Korean cyber-hacking group, was the culprit behind the highly publicised Bangladesh Central Bank heist in 2016 that diverted funds to the Philippines, Sri Lanka and other parts of Asia.[30] A North Korean cyber expert contends that Pyongyang relies heavily on foreign affiliates based in Southeast Asia to convert stolen cryptocurrency funds into fiat. Established links with over-the-counter brokers in foreign countries enable North Korean cybercriminals with money-laundering capacity to finance Kim Jong-Un's regime to develop intercontinental ballistic missiles.[31]

26 Unit 42 (2022), *2022 Unit 42 Ransomware Threat Report*, Unit 42 – Paloalto Networks, available at: https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.

27 UNODC (2022),'Darknet Cybercrime Threats to Southeast Asia', available at: https://www.unodc.org/documents/southeastasiaandpacific/darknet/index.html.

28 Ibid.

29 Seibt, S (2019), 'How cybercrime funds North Korea's nuclear programme', *France 24*, 8 August, available at: https://www.france24.com/en/20190808-cybercrime-north-korea-nuclear-programme-hacking-china-ballistic-missile.

30 Zetter, K (2016), 'That Insane, $81M Bangladesh Bank Heist? Here's What We Know', *Wired*, 17 May, available at: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know.

31 Interview with South Korean cybersecurity experts.

Terrorism and violent extremism remain imminent threats in Southeast Asia. Like other malicious actors, they are also adapting to the online environment. Cryptocurrencies offer means for illicit funds transfer, while ransomware and malware can support their strategic operations. This opens the possibility for violent extremist groups to engage with cybercriminals for weapons-related transactions.[32]

Absence of cybercrime policies and legislative gaps

UNODC contends that Southeast Asia's policy and legal gaps permit cybercriminals to evade detection from law enforcement agencies. The lack of legislative framework provides cybercriminals with a myriad of opportunities to constantly reinvent their business and operational models to maximise profit from virtual-based illicit financial flows and money laundering.[33] Although cybercrime is considered an international or transnational phenomenon, its local dimension should be equally factored into the equation. Experts interviewed in this study asserted that because of the lack or absence of policies and legislative frameworks, law enforcement agencies were prevented from increasing information sharing, conducting comprehensive investigations and facilitating cross-border co-operation.

The perceived deficiency of Southeast Asia's cybercrime legislation, combined with these debilitating technical and policy capacity gaps, make the region a safe harbour for cybercriminals. Vietnam and Malaysia stand out as the region's emerging cybercrime hubs, capturing the global–local dynamics of such illicit activity. Vietnam has a growing 'black hat' (criminal) community, supported in part by the country's strong emphasis on computing and STEM (science, technology, engineering, mathematics) disciplines. Aside from malware and fraud, most hackers are trained on intrusions to conduct data theft, BEM and financial fraud.[34] Although cybercrime and hacking are not synonymous in cybersecurity parlance, in Vietnam, cybercrime is closely linked to hacking. Prevailing corruption in the country also hampers the prosecution of cyber offenders under the full extent of the law. In the case of Malaysia, cybercriminals are not only found among the local population, but also among foreign offenders relocated to the country, most notably from Nigeria. Nigerian cybercriminals have a 'wide footprint' operating beyond West Africa, including in the US, the UK, the Netherlands, India, the Philippines and Australia. For a time, Malaysia hosted the largest number of 'expat' Nigerian fraudsters. Although the cybercrime activities in these cases are relatively low-tech scams such as BEM, the

32 Franco, J (2021), 'CENS Expert Survey on Extremism Report: Current and Emerging Threats', *RSIS*, July, available at: https://www.rsis.edu.sg/wp-content/uploads/2021/07/PR_CENSExpertSurveyOnExtremismReport_D2.pdf.

33 Ibid.

34 Lusthaus, J (2020), 'Cybercrime in Southeast Asia', *Australian Strategic Policy Institute*, available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-05/Cybercrime%20in%20Southeast%20Asia.pdf.

impacts are still damaging. Nigerian cybercriminals capitalise on local social connections to adapt and learn the local language and culture and, soon, establish possible collaborators to enhance their operations.[35]

Responses: confronting the growing threats of cybercrime

Southeast Asia's collective response to the threats of cybercrime has relied on both internal and external mechanisms designed to bolster capacity and co-ordination at the legal, policy and technical levels. This section examines the opportunities and challenges that would permit and inhibit efforts to counter cybercrime in the region, as well as prospects for peer-to-peer learning.

Opportunities

Provision of cybersecurity strategies and initiatives

Building on the ASEAN Cybersecurity Cooperation Strategy (2017–2020), ASEAN has released the Cybersecurity Cooperation Strategy 2021–2025 to outline the establishment of the ASEAN Cybersecurity Coordinating Committee, which embeds cross-sectoral collaboration on cyber issues.[36] It also established the ASEAN Ministerial Conference on Cybersecurity to tackle the growing threats of ransomware at the first substantive session of the Open-Ended Working Group on the Security of and in the Use of ICTs.[37] ASEAN has established robust cybersecurity co-operation among its key dialogue partners and other international organisations, such to improve information sharing on threats and incident response.[38] As a form of confidence building measure, the ASEAN Regional Forum developed a Points of Contact Directory for preventive diplomacy. The directory seeks to reduce the risk that misunderstanding and misperception of information and communication technology (ICT) security incidents, may lead to miscalculation and escalation if left unaddressed.[39]

35 Ibid.

36 ASEAN (2022), 'ASEAN Cybersecurity Cooperation Strategy', 26 November, available at: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

37 ASEAN (2021), 'Statement on Behalf of the Association of Southeast Asian Nations', 13 December, available at: https://documents.unoda.org/wp-content/uploads/2021/12/ASEAN-Statement-OEWG-First-Substantive-131221.pdf.

38 ASEAN (2022), 'ASEAN Cybersecurity Cooperation Strategy,' op. cit note 32.

39 ASEAN (2019), 'ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs)', ASEAN Regional Forum, March, available at: https://aseanregionalforum.asean.org/wp-content/uploads/2019/06/ANNEX-4-Comments-on-CBM1-Final-Concept-Paper-24-May-Clean.pdf.

Co-operation with multilateral bodies and institutions

On cybercrime, UNODC and Interpol have played active roles beyond awareness raising to initiate cross-border collaboration, especially among law enforcement officers, prosecutors and cybercrime inspectors. UNODC has conducted several exercises on digital forensics to strengthen national and cross-border operational capacity. Its ongoing research and capacity-building efforts are also filling the data gap regarding dark web criminality in the context of cybercrime in Southeast Asia. Through its Financial Action Task Force (FATF), UNODC is also working closely with the financial and business sector to identify chokepoints for cryptocurrencies and related money laundering services used by cybercriminals and syndicates in Southeast Asia.[40] In partnership with cybersecurity firms, Interpol has also launched various initiatives to prosecute and investigate cybercriminals that operate as part of a global crime network in the Asia Pacific. In March 2020, it established the ASEAN Cybercrime Operations Desk to enhance cybercrime intelligence and co-ordinate several multijurisdictional operations to target cybercrime.

Challenges

Diverging perceptions on ransomware

Despite the growing list of accomplishments that demonstrates Southeast Asia's agency to proactively arrest the evolving nature of cybercrime, several challenges are still on the horizon that may hamper a holistic and collective regional response. First, the region still operates on a dichotomy that tends to view ransomware through a narrow window. Debates on how to treat cybercrime – whether as a local or global phenomenon or whether it occurs purely online – are still prevalent. The Global Forum on Cyber Expertise (GFCE) argues that some governments in the region still do not consider cybercrime to be a threat.[41] This perspective is widely adopted in Southeast Asia, where the marked disparity on digital maturity among member states plus the differing views surrounding cybersecurity as a national security issue downgrade its prioritisation in actual policy implementation.[42] For instance, the cyber dimension of the South China Sea issue[43] – which often manifests through large-scale cyberespionage and/or cyber coercion – is still

40 UNODC (2022), 'Darknet Cybercrime Threats to Southeast Asia', op. cit. note 23.

41 Walsh, N (2017), 'UNODC: Countering cybercrime in Southeast Asia and beyond', *GFCE*, 21 November 21, available at: https://thegfce.org/unodc-countering-cybercrime-in-southeast-asia-and-beyond/.

42 Heinl, C (2014), 'Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime', *Asia Policy*, Vol. 18, available at: https://www.jstor.org/stable/24905282.

43 Manantan, MB (2020), 'The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea', *Issues & Studies*, Vol. 56 No. 3, available at: https://www.worldscientific.com/doi/10.1142/S1013251120400135; Gomez, MA (2013), 'Awaken the Cyber Dragon: China's Cyber Strategy and Its Impact on ASEAN', *Journal of Communication and Computer,* Vol. 10, available at: https://www.academia.edu/3082490/Awaken_The_Cyber_Dragon_Chinas_Cyber_Strategy_and_Its_Impact_on_ASEAN.

considered an 'isolated issue' and has not reached the level of national security risk.[44] Of course, doubts over ASEAN's ability to genuinely deliver its commitment on cybersecurity also looms given its diminishing credibility to demonstrate political unity.

The lack of a region-wide cybercrime framework

Second, the adoption of a region-wide cybercrime framework in the region remains elusive, in large part due to contentious political issues on the application of sovereignty in cyberspace. Aside from the Philippines, most ASEAN member states have not acceded to the Budapest Convention, an international treaty that tackles crimes committed through the internet and other computer networks.[45,46] Regionally, there is a general sense that the Budapest Convention is highly 'Western centric', owing to its roots in the European Convention on Human Rights. Each country in Southeast Asia has varying perceptions on human rights and tends to prioritise state sovereignty and non-interference. As such, codifying the treaty via domestic legislation remains a mere aspiration.[47] Despite ASEAN's adoption of the Declaration to Prevent and Combat Cybercrime, it remains to be seen if this could lead towards it crafting a regional cybercrime framework akin to the Budapest Convention under its difficult, and often painfully slow, consensus decision-making process.[48]

The lack of a streamlined regional approach on cybercrime thus presents profound implications for building cyber resilience at the strategic and operational levels. This impacts Southeast Asia's capacity to streamline efforts on information sharing and identify common grounds to enforce rules against cybercrime. To their credit, most ASEAN member states have adopted cybercrime legislation on fraud and forgery, and online child pornography; however, there remains a huge disparity in defining the conduct of criminal activities in cyberspace.[49] These disparate approaches affect ASEAN member states' ability to better co-ordinate the collection of real-time data and retain electronic evidence. In effect, law enforcement agencies face bureaucratic and legal hurdles in facilitating the preservation of stored computer data and disclosure of preserved traffic data. Additionally, establishing mutual assistance to access network servers and data

44 Interview with foreign policy experts in the Philippines.

45 Council of Europe (2022), 'Details of Treaty No. 185', 26 November, available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

46 Benincasa, E (2021), 'ASEAN needs to enhance cross-border cooperation on cybercrime', *The Strategist*, 19 January, available at: https://www.aspistrategist.org.au/asean-needs-to-enhance-cross-border-cooperation-on-cybercrime/.

47 Chen, Q (2017), 'Time for ASEAN to Get Serious About Cyber Crime', *The Diplomat*, 2 August, available at: https://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/.

48 Kono, K (2022), 'ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone', *CCDOE*, 26 November, available at: https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/.

49 Chang, LYC (2020), 'Legislative Frameworks Against Cybercrime', op. cit. note 12.

and seeking consent where possible are also impeded.[50] These realities continue to stifle genuine progress in advancing cross-border legal assistance across the region, while such assistance lies at the heart of addressing transnational threats like cybercrime.

Diverging definitions of cybercrime

Even at the multilateral level, Southeast Asian countries have yet to reach a unified position, as clearly shown during the recent deliberations at the UN to establish an international cybercrime treaty.[51] While most Western countries argue that the current Budapest Convention is working and flexible enough to adopt modifications, with the addition of protocols reflecting recent changes in the ICT landscape, Russia and China are dissatisfied with the current cybercrime treaty. Both assert that the convention's emphasis on transborder access to data and electronic evidence could impinge on national sovereignty – a perspective shared across Southeast Asia. The obvious mistrust within both camps – developing and developed economies – also colours the motivation of the ongoing negotiation, which manifests at the most fundamental level: defining cybercrime. As it stands, there is a general agreement on cyber-dependent crimes like malware and ransomware; however, there is no consensus on cyber-enabled crimes, which involve offenses that employ technology to achieve one's strategic or financial ends.[52] What makes the current rounds of deliberation even more problematic is the demand among other states, especially among developing economies, to go beyond cyber-dependent crimes. That means the inclusion of certain provisions to tackle content-related activities that may result in criminalising personal communications, online political speech, and freedom of expression and association. Among ASEAN member states, Indonesia has been the most vocal, alongside Russia and China, on including provisions on issues such as the incitement of terrorism, disinformation and hate speech.

Several civil society organisations are quick to point out that broadening the scope of the proposed treaty may inflict serious damage on fundamental human rights, particularly the freedom of expression.[53] Based on existing studies, cybercrime laws that are vaguely worded or framed in overly-broad terms have been routinely misused by governments to target dissenters.[54] Stepping into the debate, the UN Office of the High Commissioner for Human Rights (OHCHR) stressed that the inclusion of content-related offenses has been

50 Benincasa, E (2021), 'ASEAN needs to enhance cross-border cooperation on cybercrime', op. cit. note 41.

51 Walker, S (2022), 'The Quixotic Quest to Tackle Global Cybercrime', *Foreign Policy*, 11 February, available at: https://foreignpolicy.com/2022/02/11/un-cybercrime-treaty-russia-hacking/.

52 Walker, S (2022), 'The Quixotic Quest to Tackle Global Cybercrime', *Foreign Policy*,

53 Brown, D (2022), 'Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks', *Human Rights Watch*, 28 April, available at: https://www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks.

54 Human Rights Watch (2021), 'Abuse of Cybercrime Measures Taints UN Talks', 5 May, available at: https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

problematic for human rights, and should not be included in the proposed treaty.[55] The frictions underpinning the first session on the proposed cybercrime treaty resulted in a no consensus text on the objectives and scope, leaving it open. The current political gridlock on addressing cybercrime at the regional and multilateral levels presents a clear and present danger for citizens, organisations, and institutions within and beyond Southeast Asia.

Although Southeast Asia aims to maintain its neutral diplomatic stance to avoid a 'winner takes all' attitude, the current geostrategic climate is becoming untenable for its continuing desire for agency and autonomy. The diplomatic space for policy manoeuvring is shrinking due to the geopolitical competition between the US and China and the spill-over effects of Russia's unprovoked invasion of Ukraine. Mindful of these systemic risks, Southeast Asia should explore a level-headed, yet flexible, response. Hope lies on the continuing interest among states to increase technical capacity. In the short-to-medium term, training assistance will continue to bridge international co-operation. Overtime, these interventions may influence the preference, and even willingness, of countries to close the gap on the scope, intent, and purpose of a region-wide cybercrime framework in Southeast Asia.

Prospects for peer-to-peer learning

In managing the fragmentation of regional and even global co-operation, Southeast Asia could lean towards collaborating beyond its usual partners and explore other types of co-operation among similar and like-minded states who share the same experiences and interests of advancing equitable solutions to cybercrime. Technologically advanced countries like Singapore have demonstrated a strong interest towards leading cyber diplomacy efforts within and beyond the region framed around the peer-to-peer learning approach. The city-state has had its fair share of high-profile data breaches and ransomware incidents,[56] but its track record on addressing the significant gaps in cyber capacity building at the technical, policy and operational levels presents an interesting case study on peer-to-peer learning to tackle cyber-related threats like cybercrime.

Singapore tabled the formation of a working group on cybercrime during the 13th ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) in 2013. Since then, the Cybercrime Working Group has conducted relevant trainings to improve information sharing and facilitate the exchange of best practices, techniques and tools. It has also sought to engage stakeholders from law enforcement and the private sector to establish strategic partnerships.[57] In response to the sudden spike of cybercrime during the

55 UN Human Rights Office of the High Commissioner (2022), 'OHCHR key messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes', OHCHR, 17 January, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf.

56 Low, D (2021), 'Ransomware attacks threaten nations', op. cit. note 14.

57 ASEAN (2014), 'ASEAN Working Group on Cybercrime,' 27 May, available at: https://asean.org/wp-content/uploads/2021/01/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf.

pandemic, Singapore organised the Fourth ASEAN Plus Three Cybercrime Conference in 2021. As the designated ASEAN Lead Shepherd for cybercrime, Singapore held a workshop to share best practices and upgrade the competencies of law enforcement officers in the region. It also hosted the Eighth Senior Officials Roundtable on Cybercrime, which discussed new initiatives among industry partners.[58]

Outside of Southeast Asia, Singapore's engagement to improve Ghana's cybersecurity offers insights on the potential of peer-to-peer learning in cyber capacity building. During Singapore International Cyber Week 2022, Ghana's minister for communications and digitalisation revealed that she had held bilateral discussions with Singapore's minister for communications and information. The current bilateral cybersecurity co-operation focuses on critical information Infrastructure protection, regulation of cybersecurity service providers, as well as professional exchanges between officials of the Cybersecurity Agency of Singapore and the Cybersecurity Authority of Ghana. Singapore's Cyber Security Agency has been actively exchanging best practices with Ghana's Cyber Security Authority to improve its National Computer Emergency Response Team and institutionalise a multi-stakeholder approach within the Joint Cybersecurity Committee and the Industry Forum, which were established under Ghana's Cybersecurity Act 2020.

Beyond bilateral engagements, the two countries are also collaborating at the international level. Singapore has acknowledged Ghana's election to the International Telecommunications Union (ITU) Council and its support to its UN-Singapore Cyber Fellowship. Likewise, Singapore's top cybersecurity officials have also participated in Ghana's National Cybersecurity Awareness Month. Singapore and Ghana also affirmed the importance of collaborating with Interpol's Global Complex for Innovation, which is its technology branch, dedicated to improving global cybercrime response through legal assistance and digital forensics capabilities.[59]

On law enforcement, Malaysia has been actively co-operating with Interpol authorities, given the serious impact of alleged Nigerian fraudsters in the country. In October 2022, Malaysia participated in Operation Jackal, a joint law enforcement effort which targeted an international cybercrime ring known as Black Axe.[60] This West African organised crime group has been responsible for massive cyber-enabled financial crimes worldwide. In operationalising Operation Jackal, Interpol worked with law enforcement agencies to

58 ASEAN (2022), '16th ASEAN Ministerial Meeting on Transnational Crime (AMMTC) Plenary-Country Statement by Associate Professor Dr Muhammad Faishal Ibrahim, Minister of State, Ministry of Home Affairs and Ministry of National Development', Ministry of Home Affairs, 21 September, available at: https://www.mha.gov.sg/mediaroom/speeches/16th-asean-ministerial-meeting-on-transnational-crime-ammtc-plenary-country-statement.

59 Citi Newsroom (2022), 'Ghana holds bilateral meetings with Singapore to improve its Cyber security development', 25 October, available at: https://citinewsroom.com/2022/10/ghana-holds-bilateral-meetings-with-singapore-to-improve-its-cyber-security-development.

60 Interpol (2022), 'International crackdown on West-African financial crime rings', 14 October, available at: https://www.interpol.int/en/News-and-Events/News/2022/International-crackdown-on-West-African-financial-crime-rings.

deploy the Anti-Money Laundering Rapid Response Protocol (ARRP), a global stop-payment mechanism which has helped in the investigation of suspects and identification of assets.[61] In close co-ordination with Interpol's Global Financial Crime Task Force, the ARRP enabled the joint law enforcement operations to intercept illegal proceeds of crime. Malaysia's participation in Operation Jackal was crucial, given the increasing number of cybercrime-related activities of alleged Nigerian fraudsters in the country. Since 2014, US and UK authorities have also tracked down reports of malicious internet scams involving Nigerian racketeers operating in Malaysia that utilise online dating sites.[62]

Recommendations: advocating for a peer-to-peer learning approach to cybercrime

The deepening 'zero-sum game' in the current geostrategic environment makes the idea of peer-to-peer learning among small-to-medium sized states an alternative and viable mode of cyber diplomacy co-operation, especially in the interconnected world of tech. With little chance of governments coming together to compromise amid competing interests, agreeing an international cybercrime treaty remains uncertain in the foreseeable future. Countries that feel excluded from the decision-making process could band together to work on a narrow and well-defined set of functional areas of co-operation to demonstrate their agency and autonomy.

The possible cross-regional co-operation among Southeast Asia and Commonwealth countries in South Asia, Africa, Latin America and the Pacific could be a starting point to continue the discussions on cybercrime. However, co-operation across these jurisdictions will still require significant investments. Undeniably, developing economies often rely on external partners to augment resource constraints. To supplement possible resource shortages, a network of experts and practitioners specialising in cybersecurity based in think tanks, research universities and private companies could catalyse cross-border co-operation. Built around the fundamental tenets of cyber diplomacy, the following recommendations are provided to bolster Southeast Asia's collective cybercrime engagement efforts, driven by a peer-to-peer learning approach within and beyond the region.

Internal peer-to-peer learning among ASEAN member states

The first recommendation is the establishment of a cybercrime 'minilateral' grouping. The ASEAN minus X model – where some member states could opt out from the decision-making process – has become the sought-after remedy to ASEAN's declining

61 Arghire, I (2022), '75 Arrested in Crackdown on West-African Cybercrime Gangs', *Security Week*, 17 October, available at: https://www.securityweek.com/75-arrested-crackdown-west-african-cybercrime-gangs.

62 Campbell, C (2014), 'Malaysia is Becoming a Global Hub for Internet Scams Preying on the Lovelorn', 9 July, available at: https://time.com/2968765/malaysia-is-becoming-a-global-hub-for-internet-scams-preying-on-the-lovelorn.

consensus-building approach. Although in *theory* the model presents a feasible solution to the regional bloc's slow and ineffective decision-making process, its *practical* application in the field of cybersecurity would still require overcoming political sensitivities and security considerations within the group. For instance, the drawbacks of potential retaliation – through military action or economic coercion – could outweigh the perceived benefits of conducting cyber attribution against active cyber actors like China, Russia or North Korea. This presents a serious challenge to implementing a pan-ASEAN cybersecurity or cybercrime framework.

Existing 'minilateral' arrangements, such as the Indonesia-Malaysia-Philippines (INDOMALPHI) Trilateral Cooperative Arrangement that seeks to enhance maritime domain awareness in the Sulu Sea and Sulawesi Sea, could offer insights on improving cybercrime co-operation among interested parties in Southeast Asia, while circumventing the current political gridlock in ASEAN. Being the Lead Shepherd for cybercrime, Singapore could push the formation of a similar minilateral grouping on cybercrime, grounded on shared interests and principles of pragmatism. Underscoring the economic incentives of reduced costs and improved digital trade could persuade Indonesia, Malaysia, Thailand, the Philippines and Vietnam to explore the possible formation of a co-operative agreement on cybercrime, while ASEAN as a group still decides its position on how to proceed with a region-wide cybercrime framework. Such a minilateral grouping on cybercrime could pilot policy approaches on mutual legal assistance and law enforcement measures that address thorny issues such as extra-territoriality or sovereignty.

Second, institutionalising a cybercrime working group through track 1.5 dialogue – a working group composed of experts and practitioners from government, private sector, academia, and civil society – that promotes increased interaction between the public and private sector should be pursued. Interpol and UNODC's collaboration with the tech sector offer wide-ranging perspectives on incorporating private sector perspectives to manage cybercrime from the onset. Engaging the tech, financial and banking sectors within policy discussions could alleviate institutional frictions that often derail real-time legal assistance to retrieve electronic evidence or preserve data. Likewise, the private sector's technical expertise can help inform and educate government policymakers, regulators, and law enforcement officers to improve their capacity in fighting cybercrime. It is only by bringing all parties to the table – government, the private sector, academia, and civil society, all with distinct capabilities – that full-scale analysis of cybercrime as a phenomenon will take place. By obtaining an accurate picture of the cybercrime threat landscape, concerned government agencies can then prioritise and direct their resources to address cybercrime incidents based on urgency and severity.

External peer-to-peer learning with Commonwealth countries

The peer-to-peer learning model should also strengthen Southeast Asia's resolve to reinforce its connection among its counterparts in South Asia, Africa, Latin America and even the neighbouring Pacific islands. The proposed regular exchanges among these regions and countries should help preserve and cultivate an inclusive environment at the multilateral level, to reinforce trust and confidence away from the prevailing strategic manoeuvres of the big powers.

As demonstrated by the case of Singapore and Ghana, there is an opportunity for small and medium-sized countries to support each other's representation and participation in international governing bodies like the ITU. Beyond the binary narrative of the digital 'haves and have nots', small and medium-power countries should band together based on mutual and pragmatic interests to maintain the relevance and neutrality of diplomatic platforms to achieve concrete outcomes. Institutionalising track 1.5 or track 2 dialogues could be the next step to elevating the current momentum of co-operation between Southeast Asia and Commonwealth countries. Convening government policy-makers, industry practitioners, academic experts and representatives from civil society organisations could offer the opportunity for a cross-sectoral dialogue that emphasises local perspectives.

At the strategic level, Interpol and UNODC could act as brokers to lay the groundwork for greater co-operation between Commonwealth countries and Southeast Asia. With Interpol's presence in Africa and ASEAN, it can gather a consortium of Southeast Asia and Commonwealth countries to formulate confidence-building measures through information sharing through formal channels, such as the ASEAN Regional Forum. As an exploratory project, creating a Points of Contact Directory between ASEAN and Commonwealth countries may help translate this vision of peer-to-peer learning or collaboration. At the working level, organising strategic dialogues that embed tabletop exercises or 'wargames' could help test concepts and pinpoint synergies, both in heightened situations or crisis or by simulating joint law enforcement operations. In addition to promoting cyber norms and the application of international law, regular dialogues can help clarify practical considerations for small and medium-sized countries participating in peer-to-peer learning initiatives given their limited resources and capacity.

Conclusion

Southeast Asia's promise to become a digital economic powerhouse not only provides the means to fast-track its economic recovery post-COVID, but also offers the region several opportunities to shape cyber diplomacy engagements on cybercrime at the regional – and potentially at the international – levels. Through the concept of peer-to-peer learning, technologically capable states like Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam could bolster co-operation on cybercrime amid the absence of a region-wide approach and ASEAN's declining political and institutional powers.

Drawing insights from existing minilateral arrangements like INDOMALPHI can help encourage ASEAN to formulate collaborative and practical pathways to move forward in combatting cybercrime. The formation of minilateral groupings can also circumvent political deadlock and facilitate regional co-ordination and consultation on cybercrime. Operationally, such groupings could test pilot approaches on mutual legal assistance, involving law-enforcement agencies, financial regulators and cybersecurity experts – both from the public and private sectors. This concept of peer-to-peer learning can go beyond Southeast Asia and offers the region the opportunity to explore collaboration among other like-minded countries that are part of the Commonwealth and who share mutual interests in tackling cybercrime.

As international co-operation on cybercrime remains difficult, the co-operative dynamics between Southeast Asia and Commonwealth countries located in South Asia, Africa, Latin America and the Pacific could offer new ideas on cross-border co-operation on cybercrime. To make this happen, a strong network of experts and practitioners from government, the private sector, academia, and civil society will play a crucial role in designing level-headed and comprehensive exercises and initiatives to consequently influence and shape the cyber agenda at the political and technical levels of national governments. By leveraging the distinct expertise of key stakeholders from the private and public sectors in various jurisdictions through regular exchanges, it becomes plausible to analyse the evolving scale of cybercrime threats and consequently manage their risks. This will then allow governments to prioritise and direct resources that enhance cross-regional cybercrime co-operation and will especially benefit developing economies, despite the current fragmentation of global internet governance.