STIMSON

REPORT

Trade & Technology;
Cyber Program
Cyber Accountability Project

Fostering Cyber Accountability in Southeast Asia

By Mark Bryan Manantan, Ph.D.

In partnership with Canada

May 2026

ABOUT STIMSON

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

About the Author

Mark Bryan Manantan, Ph.D., is a Research Fellow at the Centre for Global Security at La Trobe University. He serves on UNESCO's AI Experts Without Borders and the advisory board of the ANU Philippines Institute. Previously, he was the inaugural Director of Cybersecurity and Critical Technologies at the Pacific Forum (Honolulu, Hawaii), where he led the Cyber ASEAN Capacity-Building Initiative (2022–2024), CONVERGE: Indo-Pacific Critical Technologies Forum (2024–2025), and the US-Japan and US-South Korea Cyber and Critical Technologies Partnerships (2020 – 2025).

Acknowledgments

This report was funded by Global Affairs Canada as part of a larger project on advancing cyber accountability in the Indo-Pacific. We are grateful to everyone who contributed views and participated in our workshop and roundtable events.

Specific thanks to our peer reviewers Anne-Marie Buzatu, Dr. Fitriani, and Pavel Mraz.

Please Cite this Publication As

Mark Bryan Manantan, 2026, *Fostering Cyber Accountability in Southeast Asia*. The Stimson Center, Washington D.C., USA.

Introduction

The cyber domain presents unique and at times daunting challenges for upholding agreed upon law and norms. Cyber threats are both persistent and omnipresent, as the technical capabilities and the tools required to generate cyber threats are widely available, and access to them is nearly impossible to control. The emergence and widespread adoption of generative artificial intelligence (GenAI) is an accelerant of the threat landscape, even as it offers important tools for cyber defense. Malicious cyber activities have thus proven difficult to manage through traditional approaches to deterrence, governance, or law enforcement. In cyberspace, behavioral norms stem from existing state obligations under international law, as well as collective and national interpretations on the application of international law. Other relevant foundations that establish guardrails for state and non-state cyber behavior include laws on cybercrime, national cybersecurity strategies, and regional policies or frameworks.

Despite these foundations, an accountability gap persists whether in adherence to law, and the subsequent introduction of appropriate and impactful consequences, or in capacities to implement measures that keep the digital ecosystem safe and secure.

Cyberspace in Southeast Asia exists in a peculiar paradox: the region includes some of the fastest-growing digital economies in the world, but the legal and institutional frameworks meant to govern that space have lagged, and capacities are uneven across the board.

This report aims to provide policy insights to support a subset of Southeast Asian countries in approaching their implementation of relevant legal frameworks and norms and to improve understanding about regional views on and approaches to cyber accountability. Its analysis is premised on the concept of cyber accountability derived from the Stimson Center's Cyber Accountability framework that essentially investigates how to improve state accountability in cyber behavior.

UNDERSTANDING CYBER ACCOUNTABILITY

The concept of cyber accountability, or rather, interest in how accountability might be strengthened in the cyber policy domain has been steadily growing in recent years. Various scholars and policy experts have contributed to a growing body of literature on the topic, at times in relation to concepts of transparency and responsible behavior.[1] Much of this research builds on other efforts to strengthen awareness and understanding of agreed behavioral norms and the applicability of international law to cyberspace, and in relation to concepts of "responsible behavior" and transparency. Understandably, research and dialogue about cyber accountability often includes consideration of technical, legal, or political cyber attribution practices.

The Stimson Center has been advancing understanding about cyber accountability through research, capacity building, and public engagement.[2] Much of this has been premised on the UN Framework for Responsible State Behavior in Cyberspace (or, the Framework) as an important baseline for state conduct in the use of ICTs, supplemented by and reflected in numerous regional and national strategies, laws, and

policies. The Framework is based on four core elements: 1) the consensus understanding that international law is applicable to state conduct in the use of ICT, as first set out by a UN Group of Governmental Experts in 2013; 2) a set of 11 non-binding, voluntary norms for state behavior focused on peacetime use of ICTs; 3) confidence-building measures (CBMs), including a set of eight CBMS articulated by a UN Open-ended Working Group on ICTs in 2024; and cyber capacity-building. The Framework is viewed as evolving and cumulative, meaning that new elements or clarifications can be considered as needed.

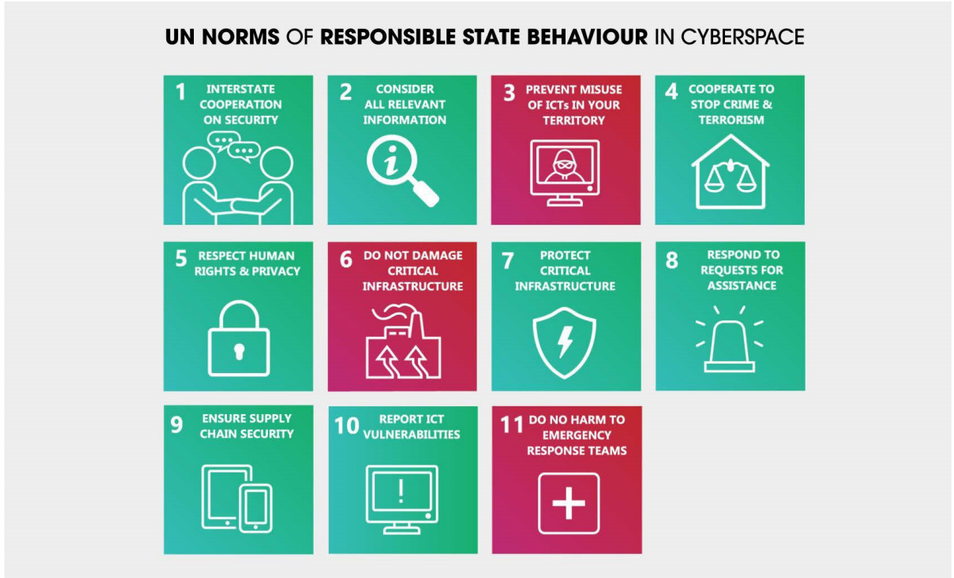

Image 1: The 11 UN Norms of Responsible State Behavior in Cyberspace[3]

Per Stimson's prior work, there are two fundamental forms of cyber accountability:

- **Negative accountability** involves the imposition of threats to coerce and raise the cost to prevent malicious behaviors, mainly through state-led efforts of attribution or the use of sanctions.

- **Positive accountability** emphasizes incentive mechanisms, policies, and instruments that encourage the fulfillment or upholding of obligations in collaboration with multiple stakeholders.

Approaching cyber accountability in both its positive and negative dimensions can provide scholars, policymakers, and practitioners with a more comprehensive and systematic approach to building cyber resilience and capacity while also holding actors to account for their malicious activities.[4] Instead of merely viewing accountability from the limited lens of threats and consequences or "who did what," it opens up an avenue to also assess what national governments and other actors require in order to uphold their commitments and undertake positive action to preserve the safety and integrity of the digital ecosystem.[5]

Stimson's research has affirmed multiple times that cyber capacity building (legal, technical, or around policy) is foundational for all aspects of cybersecurity and resilience, and therefore has a role in accountability, especially positive accountability, and can even be viewed as a form of "deterrence by denial" insofar as it builds resilience and defense.

About This Report

This report examines the opportunities and challenges facing Southeast Asia in advancing cyber accountability, and builds understanding about regional perspectives and approaches. It focuses on Cambodia, Laos, Thailand, The Philippines, and Vietnam as country case studies. These countries do not represent the entirety of Southeast Asia. However, they are ideal cases because they are in various stages towards developing cybersecurity governance mechanisms and policies and overall cyber maturity.

The report's methodology included expert interviews, email consultations, desk research, and two in-person regional events:

- The Stimson Center and ICT4Peace co-organized a regional CCB workshop in Bangkok, Thailand in April 2025 that convened representatives of multiple government agencies from Cambodia, Laos, Thailand, the Philippines, and Vietnam. The 2.5-day workshop included briefings and expert consultations featuring cybersecurity and technology policy scholars, researchers, and practitioners from industry, academia, and think tanks. To test the transfer of ideas and insights from the expert lectures and consultations, government policymakers participated in a table-top exercise (TTX) that simulated a hypothetical cyberattack. The interactive exercise informally gauged participants' knowledge and tested the practical application of the key concepts of cyber accountability.

- The initial findings of the regional workshop were presented in a closed-door roundtable event held during the 10th Singapore International Cyber Week (SICW) in October 2025.[6] The roundtable's goal was to elicit feedback on the draft findings as well as obtain deeper perspectives about cyber accountability from a broader grouping of countries. The roundtable discussion also tackled timely developments in the region, from the evolving practice of attribution and the role of the private sector in cyber incidents to the rising concerns on cybercrime and online scams.

This report is divided into three parts. Following this introduction, Section I of the report considers the unique regional context of Southeast Asia, including ASEAN-led efforts to advance implementation of the Framework, and the impact of rapid digitalization, geopolitical rivalry, and technological innovation. Section II presents a snapshot of how the five target countries are approaching norms implementation, the applicability of international law, and cyber attribution. Section III presents the report's conclusion and key policy recommendations to foster and deepen cyber accountability.

The Stimson Center is grateful to Global Affairs Canada for its support to this publication and its broader work on cyber accountability.

I. Factors Affecting Cyber Accountability in Southeast Asia

Despite its complex consensus-driven approach to managing regional affairs, ASEAN has been highly active in cybersecurity and combating cybercrime. This includes several initiatives in support of implementing the Framework. In 2018, ASEAN became the first regional organization to endorse the UN Cyber Norms in a formal way.[7] As a follow through, ASEAN developed a region-specific Norms Implementation Checklist outlining actionable steps across five pillars — policy, operational, technical, legal, and diplomacy — enabling ASEAN Member States (AMS) to more readily embed the norms in their respective national cyber strategies, policies, and regulatory frameworks.[8]

Another major milestone for ASEAN was the establishment of the regional cyber points of contact directory, a confidence-building measure under the auspices of the ASEAN Regional Forum countries that provides a direct means of communication to prevent miscalculation and escalation in the event of a major incident.[9] Recognizing the variances in digital maturity among its 10 members, ASEAN member states have been implementing cyber capacity-building initiatives to address policy and technical gaps through various channels like the ASEAN-Japan Cybersecurity Capacity-building Centre and the ASEAN-Singapore Center for Cybersecurity Excellence.

ASEAN's efforts to consolidate its cyber governance approaches were further strengthened in 2020 after the establishment of the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) to oversee all cybersecurity matters across the regional bloc's three community pillars: political-security, economic, and socio-economic.[10] Apart from enhancing policy coordination and cooperation in information-sharing, ASEAN also launched the ASEAN Regional Computer Emergency Response Team (ASEAN CERT) during the 9th ASEAN Ministerial Conference in October 2024 with the intention of strengthening regional incident response capabilities.[11]

Regional and national discussions on the application of international law are also gaining momentum. In August 2021, Singapore became the first ASEAN Member State to publish its national position,[12] followed by Thailand in July 2025.[13] Others are currently in varying stages of drafting or considering formulating their national positions. ASEAN is also finalizing the latest iteration of the ASEAN Cyber Cooperation Strategy 2026 to 2030.[14] Collectively, ASEAN is on a positive trajectory in strengthening its approach to implementing the UN Framework on Responsible State Behavior in Cyberspace and thus fostering accountability.

However, at the national level, obstacles persist among member states in consistently following through with their commitments to fostering cyber accountability due to diverging strategic, political, economic, and technological considerations. Moreover, efforts to strengthen cyber accountability across Southeast Asia are influenced by outside factors including rapid digitalization, the US-China geopolitical rivalry, and technological innovations including those brought by AI.

Rapid Digitalization

The promise of the digital economy in the post-pandemic era has accelerated the region's appetite for digitalization. The latest *e-Conomy Southeast Asia 2025* report predicts that Southeast Asia is on track to achieve $300 billion in Gross Merchandise Value with revenues reaching US$135.[15] The region's growth trajectory stems from an increasing number of internet users totaling 200 million, combined with the consistent and rising boom in e-commerce, and digital payments.[16] The drafting and expected finalization of the regionwide ASEAN DEFA in 2026 concretely demonstrates Southeast Asia's positioning as a vibrant digital ecosystem. Considered as the world's first digital economy agreement, DEFA will facilitate the region's cross-border data flow, moratorium on custom duties for electronic transmissions, and the non-discriminatory treatment of digital products and foreign source code.[17] DEFA will also exemplify ASEAN's attempt to test and implement AI-driven solutions to unlock digital payments that encourage more inclusive growth and participation of small and medium enterprises across the region.[18]

Furthermore, Southeast Asia is becoming a key hub for digital infrastructure investments such as data centers. The region's growing data center market is expected to grow with investment figures estimated at between $9 billion to $13 billion in the next few years.[19] Major trends underlining the growth prospects in the region include the rise in data consumption from 9.2. GB per user in 2020 to 28.9 GB per user in 2025; a rapid increase in cloud infrastructure demand at 33% year-over-year in 2026; the surge of e-government initiatives or the migration to the cloud to spur economic investments; and the rise of business to consumer hyper-scalers from Meta to Amazon Web Services.[20]

With expanding attack surfaces connected to rapid digitalization, nefarious cyber activities pose increasingly serious consequences to the region's thriving digital economy. The downside to Southeast Asia's digital tech drive makes it a prime target of malicious cyber-enabled activities from ransomware and online fraud to cyber-enabled scams.

Cybercrime is often perpetrated by and associated with non-state actors like organized crime syndicates, yet states also bear responsibility under the UN Convention on Transnational Crime and recently, the UN Convention Against Cybercrime.

According to the UN Human Rights Office in Bangkok, Cambodia, Laos, and Myanmar have become critical targets of and hotspots for the recent explosion of cyber-enabled fraud as linked to money laundering and illegal gambling.[21] Similarly, the UN Office on Drugs and Crime (UNODC) estimated that criminal networks targeting victims from Southeast and East Asia gained $18 billion to $37 billion USD in 2023.[22] In recent months, UNODC has raised the alarm further due to the increasing activities of transnational

organized groups engaged in online scams, and cyberfraud to support money laundering services, as well as data harvesting and disinformation.

Cybercriminals have become increasingly innovative, employing generative AI to devise more sophisticated ways to scheme victims.[23] This is particularly impactful when targeting critical infrastructure, such as seen in recent operations reportedly conducted by Anonymous VNLBN and other hacktivists affecting critical infrastructure and services in the Western provinces of Vietnam in April 2025.[24]

Ransomware also continues to be a growing challenge in Southeast Asia. In 2023, Trend Micro revealed that 52% of its global total ransomware detections targeted the region. In 2024, Kaspersky found that Southeast Asian businesses confronted approximately 135,274 ransomware attacks. This means that businesses across the region faced an average of 400 attempted attacks per day.[25] Kaspersky identified that Indonesia, Vietnam, the Philippines, Thailand, Malaysia, and Singapore were among the hardest hit of ransomware attacks.[26]

Relatedly, North Korean cyber threat actors are also operating in the region driven by their distinct geopolitical and economic motivations. In 2022, the UN Security Council Committee reports found that North Korea's Reconnaissance General Bureau controls several affiliated hacking teams — Kimsuky, Lazarus Group, and Andariel — that were involved in virtual asset theft. North Korean-sponsored hackers are known to leverage Southeast Asia for money laundering schemes to support Pyongyang's nuclear technology development program.[27] In 2024, the UNODC identified North Korean hackers involved in information-sharing among drug traffickers and fraudsters based in the Mekong region.[28] Such an activity comes as no surprise given North Korea's track record of cryptocurrency heists and high-profile ransomware attacks linked to the Lazarus Group.[29] Recently, North Korean hackers were the culprit behind the "Shrouded sleep malware campaign" through phishing emails which targeted Cambodia and other Southeast Asian countries. Once installed, the malware provides North Korean-linked hackers full access to export data or upload files.[30]

Russian-linked cyber hackers are also active in Southeast Asia in ways ranging from profit-motivated cybercriminal activities and cyberespionage to hacktivism. Cybersecurity firm Cyberfirma reported in November 2024 that Russian-based hacktivist group KyotoSh Security claimed responsibility for infiltrating a Vietnamese government website. Russian hackers are also increasingly engaged in cyber espionage in Cambodia, seeking geopolitical intelligence and sensitive information.[31] Russia's growing cyber espionage, ransomware, and financial fraud facilitated by its state-sponsored hackers or cyber mercenaries highlight its increasing presence in the region, beyond that of the U.S. and Europe.

Cyber threats have also played a small but visible role in the Thailand-Cambodia conflict, adding a digital dimension to physical tensions. In June 2025, Cambodian hacktivist group AnonSecKh launched dozens of distributed denial of service (DDoS) attacks on Thai government and military websites, prompting a rare public statement from the Thai military condemning the campaign and naming the group.[32] A month later, the KH Nightmare hack targeted Cambodian government agencies, exfiltrating hundreds of gigabytes of sensitive data.[33] These incidents, while limited in scale, signal a growing use of hack and leak operations as tools of influence and retaliation.

As the regional cyber threat landscape continues to evolve due to the rapid pace of digitalization, ASEAN's Member States (AMS) are confronted with the reality of how to best respond to the growing challenges presented by cybercrime, ransomware, and data privacy and security. Extracting accountability among state and non-state actors will demand more resources, political will, and clear guidelines to put teeth into established norms and legal frameworks. Without accountability measures in place, malicious actors will only continue to wreak havoc on the expanding threat surface.

Geostrategic Competition

Due to its strategic location and trade and economic linkages with both the U.S. and China, Southeast Asia has increasingly found itself in the throes of the ongoing geopolitical contest between the two superpowers that has increasingly manifested in the cyber domain.

Over the last decade, cyber threat assessment reports mostly from various US-based companies, alongside academic and think thank research and open-source platforms, have published extensively on the tactics, techniques, and procedures of suspected Chinese-linked state actors conducting sustained cyber-espionage campaigns against Southeast Asian countries like the Philippines, Vietnam, and Malaysia — all of whom have territorial disputes with China in the South China Sea.[34] Chinese hackers have reportedly infiltrated the computer systems and networks of government agencies and militaries to gather geopolitical intelligence relating to the South China Sea disputes, including information about government departments, academic institutions, and international organizations which have direct or indirect involvement in the protracted negotiations pertaining to the South China Sea Code of Conduct.[35] This activity is not limited to China alone, however. The 2023 leaks of Pentagon documents exposed the extent of U.S. espionage activities, even on close allies like South Korea, Israel and Ukraine, [36] as well as the use of underwater surveillance nets to siphon metadata transmitting through undersea cables in the region.[37]

As cyberspace has become a theater of great power rivalry, in which most economies and societies are increasingly dependent on both of those powers, many countries in Southeast Asia are grappling to find effective means to address the issue given the complexity of their relationship with the two powers. For instance, Chinese state-owned enterprises like Huawei and ZTE were responsible for building most of the 5G infrastructure in the region, while American firms have a wide footprint in manufacturing, as well as finance and professional services sectors that support the region's economic growth and development. Southeast Asia is walking a tightrope in navigating such multi-layered relationships, where dependence on Chinese infrastructure and U.S. capital and manufacturing creates asymmetrical vulnerabilities.

Thus, as the U.S. and China's rivalry enters uncharted territory, covert cyber operations appear likely to continue to accelerate. In the past, China has been prudent and shied away in attributing any cyber campaigns directly to the U.S. However, China's approach has very recently undergone a radical shift. In October 2025, China's Ministry of State Security claimed that the U.S. National Security Agency has stolen state secrets and conducted espionage campaigns against the National Time Service Center, a research institute that provides timekeeping services in China for national security applications.[38] The latest episode follows China's National Computer Virus Emergency Response Center's public attribution

to the U.S. of a cyberattack that infiltrated the Chinese military university, Northwestern Polytechnical University, in September 2022.

The changing cyber attribution dynamics between the U.S. and China increases the likelihood of possible escalation in already tense bilateral relations, with implications for Southeast Asia. It raises the prospects of a conflict or crisis that could advertently or inadvertently spark because of miscalculation or misinterpretation — a worst-case scenario that Southeast Asian countries will seek to avoid. Thus, this risk necessitates urgency to strengthen guardrails to manage potential conflicts.

Technological Disruption

Critical and emerging technologies like artificial intelligence (AI) and quantum computing are no longer just a means to an end in cybersecurity but have become sources of novel threats and vulnerabilities. Malicious cyber actors continue to exploit AI in augmenting traditional cyberattacks such as automated phishing, bot automation, reconnaissance, deep fakes, malware generation, domain impersonation, and so forth.[39] More recent breakthroughs like generative AI allow threat actors to engage in indirect prompt injection that can generate deliberate and planned bias into large language models, automate attacks, or compromise systems. This is likely contributing to an uptick in recent DDoS attacks against states within the region. For example, in March 2024, the Philippines House of Representatives website received 480M+ access requests, knocking it offline for hours.[40] Authorities attributed this attack to external actors, and they increased national cyber defense budgets as a result.[41] Another emerging issue is model theft where threat actors replicate an AI system's training data.[42]

The race to develop quantum technologies — computing, communications, and sensing — have serious implications for cybersecurity. Countries are increasing investments in research and development while others are also engaging in cyber espionage to strengthen their innovation edge. The "race to the bottom" surrounding quantum technologies is warranted. Quantum computers can redefine current cryptography and break widely used public key encryption algorithms, undermining digital communications and data.[43]

Policy discussions on quantum-resistant cryptography are gaining traction amid the growing number of cyber criminals engaging in Harvest Now, Decrypt Later (HNDL).[44] Although malicious actors cannot crack the encryption, they hold on to it hoping that quantum computers will soon break them.[45] Thus, the adoption of post-quantum cryptography (PQD), which can defend against cyberattacks created by quantum computers, has been growing.[46] However, adopting post-quantum cryptography (PQD) is easier said than done. Transitioning to PQD will require updating cybersecurity products, services, and protocols while also removing obsolete and vulnerable algorithms.[47]

As the pace and scope of cyber threats intensify, especially with the advent of AI and quantum computing, raising capacity and resilience in cyberspace will become even more pressing in ASEAN's portfolio. While powerful quantum computers have yet to be developed, it is crucial to be proactive and think about the implications of quantum cryptography in cybersecurity.

II. Assessing the State of Cyber Accountability in Southeast Asia

The confluence of rapid digitalization, deepening US-China strategic competition, and rapid digital transformation makes AMS more vulnerable to geopolitically motivated cyber-attacks and widespread ransomware, cybercrime, and online scams. These challenges to regional peace and stability must urge Southeast Asian policymakers to move more assuredly to implement the UN Framework. With the existing practical tools and modalities stacked in ASEAN's cyber governance toolkit, the regional bloc could exact responsibility and achieve accountability in the cyber domain.

This section outlines how the five target countries are approaching key dimensions of cyber accountability at a national level through norms implementation, legal statements, and political attribution processes or approaches. While details of some of the countries' approaches are still being contemplated or drafted, the findings below offer vital insights that sketch potential pathways on how they intend to progress in the future.

Global Cyber Norms

As noted earlier, ASEAN became the first regional organization to subscribe to UN Cyber Norms through a formal endorsement in 2018. In 2024 it developed a region-specific Norms Implementation Checklist, a strategic document outlining actionable steps that can enable ASEAN Member States to more readily embed the norms in their respective national cyber strategies, policies, and regulatory frameworks.

NATIONAL POSITIONS

In 2025, Thailand's National Cybersecurity Agency chaired the ASEAN Cyber-CC to discuss the implementation on the 11 norms within the regional bloc. For its part, Thailand has started the process of reviewing its Cybersecurity Action Plan to support the implementation of the ASEAN norms implementation checklist in collaboration with concerned agencies. It should be noted that Thailand's Cybersecurity Act, which passed in 2019, emphasizes the UN cyber norm on the protection of critical national infrastructures.[48] However, according to interviews with Thai experts and policymakers, increased public awareness among public and private sector stakeholders on the 11 norms is needed to further support their broader implementation.[49] In this regard, Thailand will also benefit from more capacity-building engagements in cyber incident response.

The Philippines has mainstreamed the 11 cyber norms through its National Cybersecurity Plan 2023 - 2028, and National Security Policy 2023 - 2028. In following the ASEAN-led norms implementation checklist, the Philippines is in the process of applying the norms but in different phases due to limited personnel and institutional capacity.[50] Further discussion about this during the Stimson-ICT4Peace workshop held in April 2025 highlighted that the Philippines has tended to prioritize norms 1 , 2 , 4, and 5, while indicating that more capacity is needed to implement norms 7 and 8. In addressing such gaps, the Philippines seeks to enhance its workforce development and strengthen the cybersecurity of its critical national infrastructure. While not strictly related to norms, another major priority for the Philippines is confidence-building measures, especially in fortifying greater public-private partnerships in threat information-sharing.[51]

Vietnam continues to adopt a top-down approach to its cybersecurity governance frameworks and initiatives. The 11 norms are supported and implemented through the National Standard for Critical Information Infrastructure, as well as various existing legal frameworks like the Cybersecurity (2018),[52] Personal Data Protection Law (2025),[53] the Law on Artificial Intelligence (2025)[54] and Decree No, 13 on Personal Data Protection.[55] The Ministry of Public Security serves as the main coordinating body of the National Cybersecurity Agency, established in 2022[56], and the National Cybersecurity Association, a multisectoral body formalized in 2020 and composed of representatives from the public and private sectors.[57] It serves as Vietnam's main focal point in coordinating and managing cybersecurity incidents. Vietnam's national CERT is under the jurisdiction of the National Cybersecurity Agency and maintains active collaboration with its international CERT counterparts to facilitate the exchange of threat information.[58]

Since ASEAN's endorsement in principle of the 11 norms in 2018, Cambodia has proactively promoted them through a range of its existing policies, strategies, and frameworks. These include Cambodia Digital Government Policy 2022 – 2035:[59] Cambodia Digital Economic and Society Policy Framework 2021 – 2035;[60] Pentagonal Strategy Phase 1 2023-2028;[61] regulatory frameworks such as Prakas on Cambodian Standard Digital Section (2021),[62] Technology Risk Management Guidelines (2019),[63] and the Sub-Decree on Digital Signature (2017)[64]. It also includes forthcoming legal instruments on cybersecurity, cybercrime, personal data protection, and on ICT and Digital Data Governance. The parliament also recently passed the country's first law dedicated to cracking down on scam centers.[65] To ensure enforcement and oversight, the Executive body, particularly the Digital Security Committee, which is chaired by the Prime Minister, with the Deputy Prime Minister as Standing vice-chair, coordinates with key representatives from four governmental bodies, namely, the Ministry of Post and Telecommunications, the Ministry of Interior, the Ministry of Defense, and the Ministry of Foreign Affairs and International Cooperations.[66]

With its relatively maturing digital economy, Laos has been embarking on a steady journey of strengthening its cybersecurity governance frameworks. Internally, it has focused on aligning cybersecurity-related initiatives with national laws and implementing cybersecurity measures in accordance with the national strategic plan. For instance, the 11 cyber norms are embedded in Laos' strategic framework, namely, the 20-year National Digital Economy Development Vision (2021 – 2040)[67] and the Cybersecurity Development Strategy (2025 – 2035).

Three government organizations are leading Laos' cybersecurity governance and initiatives. The Ministry of Foreign Affairs overseas regional and international cooperation on cybersecurity and cybercrime. Laos' National CERT under the Ministry of Technology and Communications serves as the technical point of contact and collaborates with key stakeholders from the private sector, especially domestic ICT service providers and critical national infrastructure operators. Laos CERT is also crucial in providing technical input to the Ministry of Foreign Affairs.

REGIONAL INITIATIVES

Seven years after ASEAN's endorsement of the 11 UN Cyber Norms, Cambodia, Laos, Thailand, The Philippines, and Vietnam have made positive strides in integrating many of the norms into their cybersecurity-related polices and regulatory and legislative frameworks. But upon closer examination, the awareness surrounding each norm still varies, which consequently impacts implementation. For instance, norms covering the misuse of ICTs, critical infrastructure protection, and interstate cooperation on cybercrime are widely emphasized in each country's national cybersecurity strategies and policies and legislations; in contrast, norms pertaining to human rights continue to face implementation challenges due to the socio-political and strategic context of each country. In the past, operationalizing norms on crime and terrorism, and requests for assistance, were impacted by the lack of a region-wide legal framework to effectively facilitate mutual assistance among law enforcement agencies to gather electronic evidence based on robust investigations and forensics to address cybercrime-related incidents.[68] The signing of the UN Convention Against Cybercrime, also known as the Hanoi Convention, in October 2024 offers renewed optimism towards regional cooperation on mutual legal assistance and expedited disclosure of and access to electronic evidence, including traffic data and subscriber information.[69] It is noteworthy to highlight that Cambodia, Laos, Thailand, The Philippines, and Vietnam have signed the convention.[70]

Tellingly, due to the current reconfiguration of the global manufacturing value chain, the norm surrounding supply-chain security is an emerging topic of interest among policymakers to safeguard the resilience of semiconductors and critical minerals. However, due to the low level of trust and uncertainty, amid increasing weaponization of trade and supply-chains, rallying countries to tackle such a norm may not be politically viable in the foreseeable future.

To address the uneven uptake of the cyber norms at the national level across ASEAN, Singapore supported the creation of the ASEAN norm implementation checklist in 2024 — an effort that was subsequently carried over by Malaysia in 2025.[71] As the ASEAN chair in 2025, Malaysia leveraged its leadership role to initiate development of the Regional Action Plan Matrix to support ASEAN Sectoral Bodies and Working Groups to support the implementation of the cyber norms. To further raise awareness on the checklist, the document was also endorsed during the ASEAN Digital Ministers Meeting in January 2025. Interestingly, Malaysia also noted that the checklist is a living document, and thus, implementing existing norms can go hand in hand with the development of new norms given the evolving cyber landscape.[72]

International Law

States are increasingly publishing documents containing national interpretations of how international law applies to their use of ICTs and conduct in cyberspace. As of late 2025, more than 37countries[73] and two regional blocs (the African Union[74] and the European Union[75]) have published such statements. In Southeast Asia, there is a growing consensus among policymakers and scholars that having a national position enhances their preparedness to respond to, and operate, cyber operations within the bounds of law. In clarifying the legal expectations of other parties, it establishes the redlines of unacceptable behavior and thus signals a country's resolve in confronting malicious actors should a violation of the principles have been determined. This means that it carries a "deterrent effect" because it communicates the potential consequences, including attribution or even possible retaliation, to other states. After Singapore, Thailand became the second AMS to have published a national position on the application of international law in the cyber domain, while the Philippines, Laos, Cambodia, and Vietnam have yet to formalize a process for doing so.

NATIONAL POSITIONS

In the final substantive session of the UN Open-Ended Working Group in July 2025, Thailand launched its national position on the application of international law in cyberspace covering key principles such as sovereignty and due diligence, in addition to its views on the applicability of international humanitarian law.[76] Three organizations led the process, namely the Department of Treaties and Legal Affairs under the Ministry of Foreign Affairs, the National Cybersecurity Agency, and the Ministry of Defense. The Ministry of Defense has drafted the rules of engagement concerning international humanitarian law, which are inspired by guidance from the Tallinn Manual.[77] To ensure that the process was inclusive, Thailand conducted multistakeholder consultations involving various departments and agencies of the government, alongside private sector representatives, members of academic institutions, and civil society groups. Thailand also consulted with other countries that have published their national positions, including Singapore. In applying international law during peace time, Thailand adopts a tiered approach based on its Cybersecurity Act 2019, section 60 that classifies cybersecurity threats based on three levels: non-critical, critical, and crisis.[78] While most civilian or private sector concerns are managed by the National Cybersecurity Agency, the National Security Council will be responsible for dealing with cybersecurity incidents at the crisis levels that threaten national security.[79]

At the time of publication, the Philippines has yet to begin drafting its national position on the applicability of international law in cyberspace but has expressed interest in doing so. Should the Philippine government commence the process, the primary motivation and purpose is to protect its national interests. The process would likely be spearheaded by the National Cybersecurity Inter-Agency Committee, the country's primary inter-agency body that deliberates on cybersecurity matters. The Department of Foreign Affairs, the Department of Information and Communications Technology, and the Department of Justice may lead the drafting process as the issue falls squarely within their mandates.[80] Other crucial considerations that will influence the Philippines' national position include sovereignty, territorial integrity, protection of critical national infrastructures, protection of citizens, and data privacy. To raise awareness and achieve broader support, the process will likely involve national consultations and publication of official statements.[81]

Cambodia has yet to formally begin the process of drafting its national position on the application of international law in cyberspace. Cambodian policymakers argue that various factors should be considered if such a process begins.[82] Externally, Cambodia is keen to project itself as a responsible member of the international community, aligning itself with shared norms and regional and international standards.[83] However, Cambodia must first assess internal considerations like national interests, economic benefits, social order, and political stability implications. If Cambodia pushes through, three organizations would likely lead the process: the Ministry of Justice, the Office of the Council of Ministers, and the National Assembly.[84] The King will also be involved in the ratification process. As discussions on formulating its national position in international law remain under consideration, Cambodia is focused on prioritizing confidence-building measures, capacity-building, deepening international partnerships, and raising public awareness on cybersecurity issues.[85] It also continues to participate in multilateral discussions in ASEAN and the UN. Cambodian policymakers also see the inherent advantages of engaging formal and informal intergovernmental bodies.[86]

Laos has yet to publish its official national position on international law. In the interim, policymakers in Laos continue to adopt ASEAN outcome documents/statements and frameworks. As a standard approach to any international legal convention or obligation, policymakers are reviewing and evaluating international best practices and case studies to inform the country's positioning on international law.[87] Lao PDR is placing priority on strengthening the technical capacity of its national CERT.

Vietnam has yet to publish its national position on international law. Over the past years, Vietnam has been focusing on the amendment of cybersecurity-related national legislation, strengthening diplomatic engagements, and improving internal communication channels with the public.[88] Recently, Vietnam has been recalibrating its approach to cyber policy and legislation that will have domestic and international implications. With the ongoing government restructuring that merged the Ministry of Information and Communications Technology with the Ministry of Public Security, Vietnam's 2018 Cybersecurity law is undergoing revisions to integrate the ICT law with the Cybersecurity law to strengthen national cybersecurity and enhance enforcement.[89] Under the anticipated revised law, the Ministry of Public Security becomes the primary focal point, while the Ministry of Foreign Affairs will manage the international aspects of the ICT law with the technical support provided by the Ministry of Public Security.[90]

OVERCOMING BARRIERS IN DEVELOPING A NATIONAL POSITION ON INTERNATIONAL LAW

Despite the incremental progress in the development of national positions on international law among the Philippines, Vietnam, Cambodia, and Laos, the outlook is promising due to the availability of cyber capacity-building opportunities among government policymakers offered by various international organizations, think tanks, and academic and research institutions.[91]

While prospects for publishing a national position are not far-fetched, there are a few possible obstacles and gaps to be overcome, as identified by states:

First, the prevailing bureaucratic siloing inherent in complex government structures can prevent relevant government ministries and departments from collaborating. Some countries do not have a singular dedicated government agency tasked to convene the process. Although international organizations can undertake the convening role during the earlier stages, the challenge is determining who shoulders the responsibility to shepherd the process in the long haul. Such dynamics emphasize the prevailing mistrust among government departments, ministries, and their relevant stakeholders. Overcoming the bureaucratic siloing and the absence of a central coordinating body is a prerequisite to cementing political buy-in from the government, especially from the top leadership to push through with the formal process of developing a national position, and eventually, guaranteeing its coherent implementation after its adoption.

Secondly, equally important considerations are more external and political in nature. There are perceptions among some government elites in Southeast Asia that publishing a national position may be viewed as a tacit allegiance to a Western style internet governance that embraces democratic principles and a multistakeholder approach. Another vital factor pertains to ASEAN's paradox as a regional body. Internally, there remains the underlying tension between advancing a singular and unified position to demonstrate coherence as a regional organization on one hand, and the longstanding notion of sovereignty and principles of non-interreference among member states on the other. While balancing such a tension is not unique to cybersecurity, the mounting pressures on AMS policymakers to act beyond rhetorical statements are evident because of the three drivers identified above — rapid digitalization, geopolitical competition, and technological disruptions. Some experts interviewed for this report even contend that formulating a national position will soon become an urgent priority among AMS to avoid simply subscribing to the regional position that ASEAN may develop, which could, in theory, risk sidelining national priorities. Thus, having a draft national position — whether publicly available or not — can help AMS preserve their strategic autonomy in the event that ASEAN as the regional organization puts forward a position.

Because of such considerations, international organizations seeking to build capacity have tended to adopt more entrepreneurial and tailored approaches to compel some AMS to start drafting a national position. For instance, some organizations like the United Nations Institute for Disarmament Research (UNIDIR) have conducted TTXs or scenario-based exercises to demonstrate the large-scale implications of cyberattacks against a country's major source of economic revenue or a vital critical infrastructure, and where and how international law provides protection and options for recourse.[92] Other capacity-building initiatives include activities on practical measures for states to develop a national position on international law and cyber, which have been organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the International Committee of the Red Cross, and other national and academic organizations. Additional efforts have focused on cybercrime such as online scams and ransomware. There is a capacity-building value in such exercises because they enable a country to better understand how existing international law corresponds with the realities of the cyber threats they face.

Attribution

Attribution is a foundational ingredient for accountability because it determines responsibility for wrongful action. Attribution occurs in three ways: *technical attribution*, which uses forensic investigation to identify the source of an attack; *political attribution*, which is the discretionary decision of a State to single out a certain entity, whether a State or a non-State actor, as the author of a certain cyber operation; and *legal attribution*, which determines responsibility under international law.[93]

To date, states are increasingly engaging in public attribution statements following major cyber incidents or operations, which, broadly speaking, build on technical evidence to make legal judgements and political statements.[94] In general, such statements have been more common among Western countries, with some recent notable exceptions, including China, [95] Singapore,[96] the Philippines,[97] Samoa,[98] Palau,[99] Iran,[100] and Venezuela.[101]

As mentioned, the regional CCB workshop in Bangkok employed a TTX that simulated hypothetical cyberattacks. The TTX was a central piece to the workshop because it stress tested existing attribution mechanisms or exposed the lack of such mechanisms to respond to cyberattacks. It also served as a capacity-building exercise to link attribution activities to the UN Framework. Overall, it catalyzed deeper introspection among policymakers on the importance of having a national position in international law, and relatedly, the role of attribution. Notwithstanding the fact that most Southeast Asian countries do not have formal attribution mechanisms, the goal of the TTX was to tease out how each country could likely engage (or not) in attribution during a heightened cybersecurity crisis that had region-wide implications, and to determine how states would identify which international legal principles or cyber norms were affected by the malign act in question.

After employing an interactive TTX that simulated a massive destruction to critical national infrastructures that escalated into a regional crisis requiring cooperation and possible collective attribution, what emerged was a common general approach to attribution among the five countries, which mirrors the general approach to attribution taken by many other states: *a three-pronged framework that utilizes technical, legal, and strategic factors, supported by formal and informal diplomatic channels.* Specifically, this includes the use of technical evidence to support the legal implications of cybersecurity threats, alongside strategic calculations, to determine the best channel or course of action.

While the exercise was purely informal, it did help to unpack current views, approaches, and blockages to political attribution and cooperation in addressing cyber operations. The discussion offers insights as to how Southeast Asian states can respond in the event of a major cyberattack with regional implications. Some of the anonymized and high-level findings are below:

- *Country A* recognized that publishing its national position in international law has deterrent effects because it sets the baseline for the country's institutionalized response against cybersecurity threats, especially during a major incident. However, key obstacles in the implementation of the principles in international law persist, including technical capabilities and the government's political appetite to conduct public attribution. Given such considerations, *Country A* remains highly circumspect

when dealing with cybersecurity threats. Policymakers in *Country A* contend that responding to cybersecurity incidents must be evaluated on a case-by-case basis based on a thorough triangulation of relevant technical assessments, legal frameworks and regulations, and strategic considerations. Conversely, experts in *Country A* promote and support quiet diplomacy as an effective method in remedying or resolving cyberattacks.

- *Country B* has been engaging in an ad-hoc style of attributing cyberattacks to state-sponsored hackers and hacktivists against technical, legal, and strategic considerations. Technical reports, including recommended mitigation or remediation measures, are then shared with affected agencies, as well as with law enforcement agencies, to determine if the cyber incident has breached domestic or international law. Finally, the technical and legal inputs are assessed with strategic considerations such as national security, territorial integrity, economic security, and the protection of critical national infrastructures.

- *Country B's* modus operandi in conducting public attribution involves a technical public advisory published by its National CERT. For instance, recently, the National CERT released a statement about a cyber incident which was found to be targeting government agencies in Southeast Asia in search of information related to trade and tariff measures. The attribution remained largely technical without linking it to a nation-state or contextualizing the geopolitical environment. In recent high-profile cyber incidents involving foreign hackers attempting to infiltrate *Country B's* government agencies, the National ICT Agency has exercised restraint in conducting political attribution to the foreign country in question. Despite forensic investigations that point to the hackers' command and control servers operating in the foreign country, *Country B's* government refuses to confirm the direct involvement of that government. Instead, *Country B* government officials welcome the other government's cooperation to resolve the issue.

- *Country C* does not have formal attribution mechanisms but employs and combines technical inputs, legal considerations, and strategic calculations in formulating its national response to cyberattacks. The gathering of technical inputs, which involves the identification of cybersecurity risks, data breaches, and incidents, is led by ministries that oversee ICTs, public administration, law enforcement, and defense. In determining legal recourse and repercussions, the government seeks guidance from the offices and ministries overseeing judicial issues. Finally, strategic calculations that weigh the pros and cons of responding to or attributing an attack and deciding through which channels involve ministries charged with economic affairs and foreign relations. In the case of *Country C*, it would likely attribute in an ad-hoc manner, at the discretion of country leadership, based on the technical, legal, and strategic factors mentioned.

- *Country D* also does not have any formal attribution mechanisms. During major cyber incidents, the National CERT coordinates with the national ministry tasked to identify the appropriate mitigation measures. The most recent national cybersecurity law in *Country D* outlines the specific penalties against perpetrators based on the severity and nature of unlawful acts. Some cases, such as data leakages and online scams, fall outside the remit of such laws. In those cases, *Country D's* authorities employ relevant provisions from other legislation regarding data protection, e-commerce, digital transactions, penal codes, and civil law. A national ministry deals with cyberattacks that are committed within the domestic borders, while the national CERT tackles most of the external threats through IP identification and responds accordingly. If the cyber incident has broader political, diplomatic, and socio-economic implications, authorities in *Country D* assess the situation and often address it through established diplomatic channels.

- *Country E* does not currently have any formal attribution mechanisms. However, it employs a classification approach to address cybersecurity threats based on a case-by-case basis to determine the corresponding countermeasures. In responding to cyberattacks, *Country E* stressed the integrated approach involving its key governmental cybersecurity bodies. The leading cybersecurity agency manages the technical operations of the National CERT, as well as an operations center that integrates the Critical Information Infrastructure System. Such highly integrated set-ups permit the continuous monitoring, threat prediction, and proactive prevention of cyberattacks. Furthermore, the leading agency also regularly convenes a group of key representatives from defense, public security, commerce, economy, education, and the private sector.

TESTING A REGIONAL APPROACH TO ATTRIBUTION

In tackling the regional implications of the hypothetical cyberattack during the TTX, all countries agreed on the importance of incident response and information-sharing to contain any further damage to their economies and prevent spill-over effects to other critical infrastructures. It was observed that the five countries prioritized maintaining public safety and order through timely updates regarding the incident. One country also supported confidence-building measures to diffuse potential ruptures and unintended escalation of the cyberattack.

While a collective response through joint attribution was considered, most of the countries noted that there is a prevailing trust deficit that can halt such a process. One state was also concerned about the lack of a regional approach grounded in international law, while another even downplayed the strategic utility of issuing joint statements of attribution regarding the fictional cyber incident, likely given their experience with how geopolitical divisions among member states can undermine consensus as evidenced by contentious maritime disputes, for example with the South China Sea. Such a statement underscores a simmering skepticism towards the potential role of ASEAN as a regional bloc to formulate a consolidated and concrete response during a heightened cyber crisis. Amid the pressure of addressing the fictional cyber crisis, two countries remained prudent in conducting collective attribution, emphasizing a more calibrated approach towards dialogue through informal channels.

CALIBRATED ATTRIBUTION: AN EMERGING PRACTICE?

The project's research activities and stakeholder consultations have shown that a "calibrated" approach to attribution is emerging in Southeast Asia. While not an official term, it is the author's proposal that calibrated attribution illustrates that there is not a "one size fits all" approach to cyber attribution, but rather that states, separately or together, may employ a range of tactics, both public and private. In practice, it involves calling out the malicious actor publicly but maintaining a degree of ambiguity of

who is behind it. It thus defies the conventional ambit of the highly politicized "naming and shaming" methods employed most often by the U.S. and its allies. But crucially, calibrated attribution highlights the triangulation of technical, legal, and strategic factors implemented through formal and/or informal diplomatic channels.

For example, Malaysia's Computer Emergency Response Team (MyCERT) issued a security alert in 2020 regarding a hacking campaign linked to APT40, a Chinese state-sponsored group, infiltrating Malaysian government officials. Similarly, the Philippines National Computer Emergency Response Team also issued technical reports concerning key cyber threat actors based on recorded incidents. Malaysia and the Philippines did attribute the attacks but emphasized the technical evidence rather than undertaking a political route.

Singapore's attribution of the cyber threat actor UNC3886 in July 2025 also resembled a similar approach. UNC3886 was found to have persistently targeted a wide range of critical infrastructures from energy, water, banking, finance, healthcare, transport, government, communication, and media to emergency services.[102] While Singapore's Ministry for Home Affairs called out the threat actor publicly, there was a deliberate exercise of restraint through ambiguity. Such display of calibrated attribution signaled Singapore's commitment to and resolve for upholding international law and norms in cyberspace while still mindful of averting possible diplomatic escalation should it directly chose to undertake a direct political attribution against the suspected nation-state.[103]

As shown in Southeast Asia, and possibly other regions, attribution should be conducted in a calibrated fashion supported by pragmatic actions as elaborated below:

Balancing other foreign policy and strategic priorities. The decision to undertake political attribution is one that must be balanced against numerous and at times complicated considerations tied to a country's broader relationships and priorities with the state or actor responsible for the attack. Views on attribution in the region are also deeply cultural, rooted in Asia's emphasis on restraint and harmony. States are reluctant to call out others publicly given their numerous other dependencies and relationships.

- **Emphasizing technical cooperation and capacity-building.** Beyond political attribution, there is increasing appetite for establishing a common framework on evidentiary standards that supports technical attribution. However, due to the variances in capacity, states must continue to upgrade their expertise in malware analysis and network forensics, as well as the establishment of more robust frameworks on information-sharing.

- **Leveraging diplomatic or other channels**. There is a preference to conduct attribution within established communication and relationship channels to minimize political friction with the adversary/attacking state. In this way, affected states are given flexibility to address the cyber incident in a cooperative fashion, avoiding any escalation. This is done mostly through diplomatic backchanneling, while minimizing potential frictions in the political and economic relationship with the suspected nation-state.

- **Broadening the aperture**. Emerging instances of calibrated attribution allow for expansion of cyber accountability. In addition to state responsibility, accountability also rests with relevant private sector actors, a point that was stressed often throughout the roundtable and workshop. As policymakers note, most computer networks and systems are operated by third-party contractors that have full-visibility and access; therefore, such companies share the burden for accountability and building resilience against future incidents in collaboration with government and civil society.

- **Region-wide good practice**. Calibrated attribution practices may facilitate region-wide attribution practices or standards, or other important forms of cooperation. Several experts emphasized that this can be pursued under the ASEAN-CERT to consolidate efforts among existing national CERTs in the region that are already conducting technical attribution.

III. Fostering Accountability: Conclusion and Policy Recommendations

This report has reviewed how five Southeast Asian countries are approaching the implementation of global norms, international law, and attribution capabilities, as part of a broader understanding about cyber accountability gaps, needs, and approaches in the region.

To capitalize on the positive momentum of Southeast Asia, the report offers the following recommendations:

- **Implement targeted and tailored CCB to address context-specific needs and gaps** of AMS to further advance cyber accountability. ASEAN and its dialogue partners through the ASEAN CC, as well as the ASEAN-Japan Cybersecurity Capacity-building Centre and the ASEAN-Singapore Center for Cybersecurity Excellence, should redouble efforts towards conducting targeted CCB on topics and in ways that raise technical and policy knowledge and awareness, including towards common understandings and approaches on the negative and positive dimensions of cyber accountability.

- **Support and encourage efforts of governments in the region to establish a national position on the application of international law in cyberspace**. Doing so helps to establish and further deepen common understanding about how existing international law is interpreted and applied to state conduct in the use of ICTs, which is important for accountability, transparency, and predictability amid heightened geopolitical tensions and proliferation of novel cyber threats and vulnerabilities.

- **Fast-track the operationalization of the ASEAN-CERT**. Because most of the countries still lack formal attribution mechanisms, enhancing regional information-sharing in both crisis and non-crisis situations will become even more crucial. Another platform worth engaging in region-wide information-sharing and incident response is the Asia Pacific-CERT. National CERTs must maximize their linkages to both organizations.

- **Establish a roster of national experts to support countries' progress in implementing the ASEAN Norms Implementation Checklist**, and stock-taking on confidence-building measures. ASEAN should increase peer-to-peer learning opportunities to share best practices with stakeholders, especially those in the private sector, on core aspects of cyber accountability. For instance, in discussing public-private partnerships in cybersecurity, AMS are encouraged to make use of the checklist and use relevant convenings to report against their progress in norms implementation and enhance threat information-sharing.

- **Develop a strategic roadmap to guide the development of collective statements or joint efforts in the event of cyber crises that can affect multiple countries in the region.** Establishing a standing committee on possible joint-cyber attribution at the ASEAN-Regional Forum can be an initial step on advancing dialogue on common evidentiary standards for making technical attributions. This can be added as part of the region's CBM that builds on the Points of Contact Directory.

- **Donor countries and non-governmental partners are encouraged to adopt a priority-based approach to CCB to improve coordination and maximization of resources.** Establishing a CCB clearinghouse or leveraging existing platforms like the Global Forum on Cyber Expertise (GFCE) to support the optimization of resources and avoid waste and inefficacy could be a useful tool for preventing the duplication of initiatives and encouraging greater maximization of public-private partnerships. Amid resource constraints, CCB should be directed to countries with the greatest need for sustained capacity-building support.

As ASEAN elevates its digital ambitions with the highly anticipated conclusion of the Digital Economic Framework Agreement in 2026, the notion of cyber accountability becomes even more pressing to ensure that every stakeholder in the public and private sectors upholds their commitments and contributes to the formation of a secure and interoperable regional tech ecosystem that minimizes malicious efforts that can disrupt the smooth flow of digital trade and data across borders. With continuous, targeted, and contextualized approaches to cyber capacity-building, Southeast Asia can enhance coordination, build trust, and strengthen both the policy and practice of accountability.

Endnotes

1 Allison Pytlak and James Siebens, eds., July 2024, Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches. The Stimson Center, Washington D.C., USA.

2 Stimson Center. "Cyber Accountability." *Stimson Center*, December 16, 2025. https://www.stimson.org/project/cyber-accountability/.

3 "Now That ASEAN Has Its Cyber Norms Checklist, the Hard Work Begins." The Strategist, Australian Strategic Policy Institute, date not listed. https://www.aspistrategist.org.au/now-that-asean-has-its-cyber-norms-checklist-the-hard-work-begins/.

4 Allison Pytlak and James Siebens, eds., July 2024, Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches. The Stimson Center, Washington D.C., USA.

5 Patryk Pawlak, "Accountability in Cyberspace: The Holy Grail of Cyber Stability?" *Policy Brief*, EU Cyber Direct, Leiden University Institute of Security and Global Affairs, March 2024, https://www.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/isga/accountability-in-cyberspace-patryk-pawlak-march-2024.pdf.

6 Singapore International Cyber Week. "Cyber Accountability in Asia: Navigating Norms and Legal Frameworks." *SICW*, 2025. https://www.sicw.gov.sg/events/22-oct/cyber-accountability-in-asia-navigating-norms-and-legal-frameworks/.

7 ASEAN. *ASEAN Cybersecurity Cooperation Paper 2021–2025*. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

8 ASEAN. *ASEAN Cyber Norms Checklist*. 2025. https://asean.org/wp-content/uploads/2025/02/ASEAN_checklist_print.pdf.

9 Australian Government, Department of Foreign Affairs and Trade. "Building Confidence in Cyberspace Through the Development of a Regional Cyber Points of Contact Directory." *DFAT*, May 20, 2019, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/building-confidence-in-cyberspace-through-the-development-of-a-regional-cyber-points-of-contact-directory.

10 Association of Southeast Asian Nations, "Joint Media Statement of the 19th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings," October 25, 2019, p. 2, https://asean.org/wp-content/uploads/2021/09/ADOPTEDTELMIN-19th-TELMIN-JMS-.pdf; Association of Southeast Asian Nations, *ASEAN Cybersecurity Cooperation Paper 2021–2025* (2022), https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

11 Cyber Security Agency of Singapore. "Establishment of ASEAN Regional Computer Emergency Response Team (CERT)." October 20, 2024. https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region/.

12 United Nations General Assembly. *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266*. A/76/136. July 13, 2021. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

13 Thailand, Ministry of Foreign Affairs. *Thailand's National Position on Responsible State Behaviour in Cyberspace*. July 2025. https://image.mfa.go.th/mfa/0/6p4M7ae5k9/Thailands_NP_JUL2025_.pdf.

14 U.S. Department of State. "Co-Chairs' Statement on the 6th U.S.-ASEAN Cyber Policy Dialogue." October 2025. https://www.state.gov/releases/office-of-the-spokesperson/2025/10/co-chairs-statement-on-the-6th-u-s-asean-cyber-policy-dialogue.

15 Temasek, Google Cloud, and Bain & Company. "E-Conomy SEA 2025 Report: ASEAN's Digital Economy Poised to Surpass $300 Billion." 2025. https://www.temasek.com.sg/en/news-and-resources/news-room/news/2025/e-conomy-sea-2025-report-aseans-digital-economy-poised-to-surpass-300-billion.

16 Ibid.

17 ASEAN. "ASEAN DEFA Study Projects Digital Economy Leap to US$2tn by 2030." *ASEAN*, 2025. https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/.

18 Suominen, Kati. "How Would the DEFA Add Value to Asia-Pacific Trade?" *White Paper*. Singapore: Hinrich Foundation, September 10, 2024. https://www.hinrichfoundation.com/research/wp/ftas/how-would-the-defa-add-value-to-asia-pacific-trade.

19 Bhaskar Rakshit, Carlos Oliver Mosquera, Varun Arora, and Carlo Celis, "How Data Center Operators Can Win in Southeast Asia," A.T. Kearney, November 11, 2022, https://www.kearney.com/service/digital-analytics/article/-/insights/how-data-center-operators-can-win-in-southeast-asia (no currency provided for referenced statistics).

20 Ibid.

21 United Nations Human Rights Office of the High Commissioner for Human Rights, Regional Office for South-East Asia. "Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response." Bangkok: OHCHR, 2023. https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf.

22 United Nations Office on Drugs and Crime (UNODC), Regional Office for Southeast Asia and the Pacific. "Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape." October 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

23 United Nations Office on Drugs and Crime (UNODC). "Crushing Scam Farms: Southeast Asia's 'Criminal Service Providers'." July 11, 2024. https://www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms--southeast-asias-criminal-service-providers.html.

24 Geenens, Pascal. "Cyber Assault on Vietnam: Inside the 2025 Attacks by Anonymous VNLBN." *Radware* (blog). April 29, 2025. https://www.radware.com/blog/threat-intelligence/cyber-assault-on-vietnam-by-anonymous-vnlbn/.

25 Knowles, Catherine. "Southeast Asian Firms Face Surge in Ransomware Attacks in 2024." *SecurityBrief Asia*, April 17, 2025. https://securitybrief.asia/story/southeast-asian-firms-face-surge-in-ransomware-attacks-in-2024/.

26 China Daily Hong Kong. "SE Asian Businesses Face 400 Ransomware Attacks Daily." May 8, 2025. https://www.chinadailyhk.com/hk/article/611263.

27 U.S. Department of the Treasury. "Treasury Sanctions DPRK Bankers and Institutions Involved in Laundering Cybercrime Proceeds and IT Worker Funds." Press release SB0302. November 4, 2025. https://home.treasury.gov/news/press-releases/sb0302.

28 Wilson, Tom. "North Korean Hackers, Criminals Share Money Laundering Networks in Southeast Asia: UN." *Reuters*, January 15, 2024. https://www.reuters.com/world/asia-pacific/north-korean-hackers-criminals-share-money-laundering-networks-southeast-asia-un-2024-01-15/.

29 U.S. Department of the Treasury. "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups." Press release SM774. September 13, 2019. https://home.treasury.gov/news/press-releases/sm774.

30 Greig, Jonathan. "North Korea 'Shrouded Sleep' malware campaign targeting Cambodia." *The Record*, October 3, 2024. https://therecord.media/north-korea-malware-espionage-cambodia.

31 Cyfirma. "The Changing Cyber Threat Landscape: Southeast Asia." November 29, 2024. https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-southeast-asia-2/.

32 Reddick, James. "Pro-Cambodian hacktivists launch attacks on Thai government sites amid border dispute." *The Record*, June 17, 2025. https://therecord.media/pro-cambodian-hacktivists-target-thai-websites-amid-border-dispute.

33 Nation Thailand. "Thailand Strengthens Cybersecurity Defences among 1.5 Million Servers under Constant Monitoring." July 31, 2025. https://www.nationthailand.com/news/general/40053423.

34 Pacific Forum, "Cyber Threat Tracker," *Cyber ASEAN*, https://cyberasean.pacforum.org/cyber-threat-tracker; Council on Foreign Relations, "Cyber Operations Tracker," https://www.cfr.org/cyber-operations/.

35 Manantan, Mark Bryan. "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea." *Issues & Studies* 56, no. 03 (September 2020): 2040013. https://doi.org/10.1142/s1013251120400135; See the October 2024 attacks on Thailand 's government institutions here: Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents Since 2006*, updated June 2025, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-06/250610_Significant_Cyber_Incidents.pdf?VersionId=IAAkHurCCF.s7dd26zpWQUXbumz3JXsq; March 2023 attacks against Viet Nam, Thailand, and Indonesia here: Greig, Jonathan. "Chinese Military Hackers 'RedHotel' Target Countries across Asia, North America, Europe." *The Record*, August 8, 2023. https://therecord.media/chinese-military-hackers-redhotel-target-countries-across-asia-north-america-europe; February 2023 attacks on telecommunications and media firms in Viet Nam here: Trend Micro. "Earth Zhulong: Familiar Patterns Target Southeast Asian Firms." February 8, 2023. https://www.trendmicro.com/en_us/research/23/b/earth-zhulong-familiar-patterns-target-southeast-asian-firms.html., and the compromise of Philippine government networks in November 2023 here: Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents Since 2006*, updated June 2025, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-06/250610_Significant_Cyber_Incidents.pdf?VersionId=IAAkHurCCF.s7dd26zpWQUXbumz3JXsq.

36 Bertrand, Natasha, and Kylie Atwood. "Highly Classified Pentagon Documents Leaked, Showing US Spying on Allies and Foes." *CNN*, April 10, 2023. https://edition.cnn.com/2023/04/09/politics/pentagon-leaked-documents-us-spying-allies-foes.

37 Noor, Elina. "Subsea Communication Cables in Southeast Asia: A Comprehensive Approach Is Needed." Carnegie Endowment for International Peace, December 18, 2024. https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables?lang=en.

38 Martin, Alexander. "China Attack National Time Center." *The Record*, October 20, 2025. https://therecord.media/china-attack-national-time-center.

39 Microsoft. *Microsoft Digital Defense Report 2025*. 2025. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

40 Philippine News Agency. "541.7M Cyberattacks on Congress Website Repelled." March 13, 2024. https://www.pna.gov.ph/articles/1220820.

41 Lavrova, Darya. "Cybersecurity Threatscape in Southeast Asia." Positive Technologies, March 20, 2025. https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-in-southeast-asia/.

42 Microsoft, *Digital Defense Report 2025*.

43 Microsoft, *Digital Defense Report 2025*.

44 KPMG Australia. *Securing Tomorrow: Strategic Compliance in the Quantum Age*. 2024. https://assets.kpmg.com/content/dam/kpmgsites/au/pdf/2024/securing-tomorrow-strategic-compliance-in-the-quantum-age.pdf.coredownload.inline.pdf.

45 National Institute of Standards and Technology. "What Is Post-Quantum Cryptography?" Last modified February 27, 2026. https://www.nist.gov/cybersecurity/what-post-quantum-cryptography.

46 Ibid.

47 National Institute of Standards and Technology. "Post-Quantum Cryptography Standardization." Computer Security Resource Center. https://csrc.nist.gov/projects/post-quantum-cryptography.

48 Interview with Thai policymakers, Bangkok, April 2025.

49 Ibid.

50 Interview with Filipino policymakers, Bangkok, April 2025.

51 Ibid.

52 Interview with Vietnamese policymaker, Bangkok, April 2025; Vietnam, National Assembly, *Law on Cybersecurity*, Law No. 24/2018/QH14, June 12, 2018, art. X, https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf.

53 Vietnam, National Assembly, *Law on Personal Data Protection*, Law No. 91/2025/QH15, June 26, 2025, https://dpo-india.com/Resources/Privacy_Regulations_in_Asia_Pacific_Countries/Vietnam-Personal-Data-Protection-Law(PDPL)26.06.25-Law-No.91-2025-QH15.pdf.

54 National Assembly of Vietnam. Law No. 134/2025/QH15 on Artificial Intelligence. Hanoi, December 10, 2025. https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Law-134-2025-QH15-Artificial-Intelligence/689735/tieng-anh.aspx.

55 Vietnam, Government, *Decree 13/2023/ND-CP on Personal Data Protection*, April 17, 2023, https://resources.finalsite.net/images/v1710749328/saigon/l5cqb4izgsc1uwugo98e/Decree13_2023_ND-CPPersonalDataProtectionENGLISH.pdf.

56 Vietnam, Ministry of Public Security. "National Assembly Passes Law on Cybersecurity." October 12, 2025. https://en.bocongan.gov.vn/article/national-assembly-passes-law-on-cybersecurity-1765507574.

57 National Cybersecurity Association (NCA). "Home." Accessed April 7, 2026. https://nca.org.vn/home?l=en.

58 Ministry of Science and Technology, Vietnam. "Cybersecurity Emergency Response Center Established." *MST.gov.vn*, October 14, 2019. https://english.mst.gov.vn/cybersecurity-emergency-response-center-established-197139865.htm.

59 Ministry of Post and Telecommunications. *Cambodia Digital Government Policy 2022-2035*. Royal Government of Cambodia, January 2022. https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf.

60 Supreme National Economic Council. *Cambodia Digital Economy and Society Policy Framework 2021-2035*. Royal Government of Cambodia, Ministry of Post and Telecommunications, May 2021. https://asset.cambodia.gov.kh/mptc/media/EN-Policy-Framework-of-Digital-Economy-and-Society.pdf.

61 Royal Government of Cambodia. *Pentagonal Strategy - Phase I for Growth, Employment, Equity, Efficiency, and Sustainability: Building the Foundation Towards Realizing the Cambodia Vision 2050*. Phnom Penh, August 2023. https://faolex.fao.org/docs/pdf/cam222534.pdf.

62 Consumer Protection, Competition and Fraud Repression Directorate-General (CCF). "Prakas." *Laws & Regulations*, Ministry of Commerce, Kingdom of Cambodia, https://www.ccfdg.gov.kh/en/laws-regulations/prakas/. Accessed April 7, 2026.

63 National Bank of Cambodia (NBC). *Technology Risk Management Guidelines*. Phnom Penh, July 2019. https://www.nbc.gov.kh/download_files/publication/itguideline_eng/NBC-Risk-Management-Guidelines-July%202019.pdf.

64 Royal Government of Cambodia. *Sub-Decree No. 246 on Digital Signatures*. Ministry of Post and Telecommunications, Phnom Penh, February 7, 2022. https://asset.cambodia.gov.kh/mptc/media/2022/02/7-Digital-Signature-English.pdf.

65 Lach, Chantha. "Cambodian Parliament Passes Landmark Cybercrime Law After Scam Centre Scrutiny." Reuters, April 3, 2026. https://www.reuters.com/world/asia-pacific/cambodian-parliament-passes-landmark-cybercrime-law-after-scam-centre-scrutiny-2026-04-03/.

66 UNIDIR Cyber Policy Portal. "Cambodia." *Cyber Policy Portal*. United Nations Institute for Disarmament Research (UNIDIR), accessed April 7, 2026. https://cyberpolicyportal.org/states/cambodia.

67 Ministry of Technology and Communications. *20-Year National Digital Economy Development Vision (2021-2040), 10-Year National Digital Economy Development Strategy (2021-2030), 5-Year National Digital Economy Development Plan (2021-2025)*. Lao People's Democratic Republic, Vientiane, December 2021.

68 Manantan, Mark Bryan. "Cyber Diplomacy and Co-operation on Cybercrime between Southeast Asia and Commonwealth Countries." *Commonwealth Cybercrime Journal*, Volume 1. London: The Commonwealth, 2022. https://thecommonwealth.org/publications/commonwealth-cybercrime-journal-volume-1/cyber-diplomacy-co-operation-cybercrime-between-southeast-asia-and-commonwealth-countries.

69 United Nations (UN). *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*. Adopted December 24, 2024. Vienna: United Nations Office on Drugs and Crime (UNODC), 2024. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html.

70 United Nations Office on Drugs and Crime (UNODC). *Full List of Signatories on 25 and 26 October 2025 (72 Signatories): United Nations Convention against Cybercrime*. Vienna: UNODC, October 2025. https://www.unodc.org/res/cybercrime/convention/Full_List_of_Signatories_on_25_and_26_October_2025_72_signatories_UN_Convention_against_Cybercrime.pdf.

71 Cyber Security Agency of Singapore (CSA). "Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region." *CSA Press Releases*, October 16, 2024. https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region/.

72 Interview with cybersecurity expert, Singapore, November 2025, https://estatements.un.org/estatements/12.1255/20250218100000000/aVtJXlzBMbQ/DVcDG-jJ_nyc_en.pdf.

73 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). "Applicability of International Law." *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Cyber Law Wiki*. Tallinn, Estonia: CCDCOE. https://cyberlaw.ccdcoe.org/wiki/Applicability_of_international_law.

74 African Union (AU), Peace and Security Council. *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in the Cyberspace*. Communiqué PSC/PR/COMM.(CXCXVI), adopted January 29, 2024. Addis Ababa: African Union, 2024. https://cms.cyberpolicyportal.org/uploads/CAP_Communiques_FULL_0e34eb5799.pdf.

75 Council of the European Union. *Declaration on a Common Understanding of International Law in Cyberspace*. Document ST-15833-2024-INIT. Brussels, November 18, 2024. https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf.

76 Permanent Mission of Thailand to the United Nations. "Thailand Launched its First National Position on the Application of International Law in Cyberspace." *Royal Thai Embassy, New York*, July 8, 2025. https://unmissionnewyork.thaiembassy.org/en/content/thailand-launched-its-first-national-position-on-t?cate=67d47fd37ed649136a7c8093; Kingdom of Thailand, Ministry of Foreign Affairs. *Thailand's National Position on the Application of International Law in Cyberspace*. Bangkok, July 2025. https://image.mfa.go.th/mfa/0/6p4M7ae5k9/Thailands_NP_JUL2025_.pdfe.

77 Interview, Thai policymakers, Bangkok, April 2025

78 Kingdom of Thailand. *Cybersecurity Act B.E. 2562 (2019)*. Bangkok: Ministry of Digital Economy and Society, 2019. https://cc.kmutt.ac.th/Files/Act%20Eng/cybersecrutiy-act-2019-en.pdf.

79 Ibid.

80 Interview, Filipino policymaker, Bangkok, April 2025.

81 Interview, Filipino policymaker, Bangkok, April 2025.

82 Interview, Cambodian policymaker, Bangkok, April 2025.

83 Ibid.

84 Ibid.

85 Ibid.

86 Ibid.

87 Interview, Laotian policymakers, Bangkok, April 2025.

88 Interview, Vietnamese policymaker, Bangkok, April 2025.

89 Ibid.

90 Ibid.

91 UNIDIR Security and Technology Programme. *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT*. United Nations Institute for Disarmament Research (UNIDIR), Geneva, May 2024. https://unidir.org/wp-content/uploads/2024/05/UNIDIR_A_Compendium_of_Good_Practices_Developing_a_National_Position_on_the_Interpretation_of_International_Law_and_State_Use_of_ICT.pdf; Mačák, Kubo, Talita Dias, and Ágnes Kasper. *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), May 2025. https://ccdcoe.org/uploads/2025/05/Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf.

92 UNIDIR Security and Technology Programme, *Compendium of Good Practices*, 18

93 CCDCOE. "Attribution." *NATO Cooperative Cyber Defence Centre of Excellence Cyber Law Wiki*, Tallinn, Estonia. https://cyberlaw.ccdcoe.org/wiki/Attribution.

94 Singh, Virpratap Vikram. "Reframing Cyber Attribution." *Charting Cyberspace*, International Institute for Strategic Studies (IISS), December 18, 2025. https://www.iiss.org/online-analysis/charting-cyberspace/2025/12/reframing-cyber-attribution/.

95 Saarinen, Juha. "Chinese Researchers Attribute Top-Tier Backdoor to NSA Equation Group." *iTnews*, February 25, 2022. https://www.itnews.com.au/news/chinese-researchers-attribute-top-tier-backdoor-to-nsa-equation-group-576528.

96 Abdul Rahman, Muhammad Faizal bin. "As Cyber Threats Grow, Singapore Walks a Careful Line on Identifying State Actors." RSIS, July 29, 2025. https://rsis.edu.sg/rsis-publication/rsis/as-cyber-threats-grow-singapore-walks-a-careful-line-on-identifying-state-actors.

97 National CERT Philippines. "HazyBeacon Backdoor Observed in Attacks against Southeast Asian Government Agencies." July 16, 2025. https://www.ncert.gov.ph/2025/07/16/hazybeacon-backdoor-observed-in-attacks-against-southeast-asian-government-agencies/.

98 Dziedzic, Stephen. "China-backed APT40 blamed for cyber attacks on Samoa." *ABC News*, February 11, 2025. https://www.abc.net.au/news/2025-02-12/china-backed-apt40-blamed-for-cyber-attacks-on-samoa/104927412.

99 Judah, Jacob. "A Pacific Island With Ties to Taiwan Was Hacked. Was It Political?" *The New York Times*, June 2, 2024. https://www.nytimes.com/2024/06/02/world/asia/palau-taiwan-china-hack.html.

100 BBC. "Stuxnet worm hits Iran nuclear plant staff computers." March 4, 2011. https://www.bbc.com/news/technology-12633240.

[101] Lillis, Katie Bo, Sean Lyngaas, and Kylie Atwood. "Maduro Cyberattack Trump CIA." *CNN*, October 29, 2025. https://edition.cnn.com/2025/10/29/politics/maduro-cyberattack-trump-cia.

[102] Reuters. "Singapore Says Cyber Espionage Group Targeting Critical Infrastructure." July 18, 2025. https://www.reuters.com/world/china/singapore-says-cyber-espionage-group-targeting-critical-infrastructure-2025-07-18/.

[103] Feakin, Tobias. "Calibrated Signals: How Middle Powers Are Rewriting the Rules of Cyber Attribution in the Indo-Pacific." *The Diplomat*, August 9, 2025. https://thediplomat.com/2025/08/calibrated-signals-how-middle-powers-are-rewriting-the-rules-of-cyber-attribution-in-the-indo-pacific/.

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

STIMSON.ORG

STIMSON

INNOVATIVE IDEAS CHANGING THE WORLD