# 4.3. Varied Threats, Tailored Responses: Rethinking International Cyber Cooperation in Southeast Asia

*Surachanee 'Hammerli' Sriyai*
*Se&I Strategic Advisory*

## *4.3.1. Introduction*

On 25 October 2025, 72 UN Member States signed the United Nations Convention against Cybercrime (UNCC) in Hanoi, Vietnam, underscoring their commitment to fight against the global problem of cybercrime.[1] With the transnational nature and impact of the crime, international cooperation in cybersecurity is no longer optional; it has become an imperative. Beyond the new Convention, international cooperation in cybersecurity has become ever more prominent in Southeast Asia, a region identified as hotspot for scam operations and IT-enabled illicit activities. Globally, scam losses are estimated to amount to hundreds of billions of US-Dollars, with figures in 2025 reports suggesting around 442 billion US-Dollars of losses. In the United States, an estimated 4.4 billion US-Dollars has been attributed to so-called 'pig butchering' schemes, a tactic most prevalent in Southeast Asia.[2]

For external partners, this illustrates both the promise and complexities of engagement. Since 2017, the Japanese Government has funded the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) hosted in Bangkok with a goal to build competency for cybersecurity experts in the public and critical information infrastructure (CII) sectors of ASEAN countries.[3] In August 2021, the US Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber Security Agency of Singapore (CSA) signed a Memorandum of Understanding to expand cooperation on information-sharing, joint exercises, and research on critical technologies.[4] Similarly, in November 2024, the United States and Vietnam concluded a cooperation agreement to strengthen Vietnam's digital infrastructure resilience and capability to counter cyber threats.[5] More broadly, in October 2024, the Philippines has agreed to collaborate with the United States and Japan to enhance the nation's cyber and digital resilience through the US-Japan-Philippines Trilateral cyber and digital dialogue, which took place

on the side-lines of the 9th Singapore International Cyber Week.[6] For collaboration with European counterparts, compelling examples include the regional workshop on cybercrime and electronic evidence organised by the Council of Europe in Bangkok under the "Octopus Project", where more than 50 criminal justice representatives from Southeast Asian countries participated. The aim was to align legislative frameworks, enhance technical capacities for electronic evidence, and foster networking across jurisdictions.[7] Another recent instance of cooperation is Operation SECURE, which is a joint initiative of the European Union, the Council of Europe, and INTERPOL's Cybercrime Directorate-Asia and South Pacific Desk. The event was held in Bangkok in late February 2025 and brought together 75 professionals from 22 countries, including major regional partners and industry. The agenda included simulated responses to malware and "infostealer" threats, tabletop exercises on cross-border incident management, and sharing of best practices on transnational cybercrime.[8] These real-world initiatives reflect the earnest efforts of external stakeholders to build resilience, share best practices and foster partnerships in Southeast Asia.

Despite the commendable nature of such cooperation, two important caveats must be acknowledged. First, while many programmes place the emphasis on combating cybercrimes and threats committed by nonstate actors (e.g., scams, fraud, phishing, malware), these threats are only one part of the cyber threat spectrum in the region. State-linked intrusions, supply chain compromise, ransomware against critical infrastructure, geopolitical cyber-coercion and peer-state espionage are equally material but may receive less emphasis when creating an agenda which focuses on building the capacity to combat cybercrime. Second, extrapolating best practices from Western or more developed cyber ecosystems and transplanting them into Southeast Asia without adjustment can overlook significant variations: partner states differ in legal frameworks, institutional capacity, threat-profiles, political incentives, and strategic priorities. What works in a mature American or European cyber environment may falter when applied to a Southeast Asian state dealing with limited digital infrastructure, nascent mutual-legal-assistance regimes, or different threat vectors (such as scam-centres tied to forced labour or cross-border insurgent networks). Recognising that variation is essential if cooperation is to be effective, sustainable and well-aligned with local realities.

With that backdrop, this paper explores Southeast Asia's cyber threat landscape against variations that exists from outside the region, and how

it may shape opportunities for cooperation. Relying primarily on the data from the Council on Foreign Relations (CFR)'s Cyber Operations Tracker (2025) that records all publicly disclosed incidents of cyber activities around the world that can be attributed to state-sponsored actors since 2005, this paper takes a state-centric approach, viewing Southeast Asian countries as both targets and perpetrators of cyber operations.[9] Since the data exclusively includes cases where the attacker, often referred to as the threat actor, is believed to have connections with a nation-state, its emphasis on state-linked operations is an added value to this analysis as it highlights instances where governments or their proxies engage in cyber activities to advance their foreign policy objectives, sifting out the non-attributable attacks by nonstate actors, that tend "to be murkier and makes for less reliable data" or may have already been extensively discussed elsewhere. Later, this paper will turn to concrete recommendations for EU countries, and in particular Germany, to expand collaboration with Southeast Asia in cybersecurity.

### *4.3.2. Cyber Threats in Southeast Asia and Comparative Variation*

In Southeast Asia, cyber threats manifest along multiple, often overlapping axes. First, organised-crime networks exploit weak oversight and high connectivity to mount large-scale fraud, online-scams and money-laundering operations. Simultaneously, advanced persistent threat (APT) campaigns targeting governments, infrastructure and industry exploit uneven patching practices and regional vendor ecosystems. Finally, the rapid growth of cloud, digital economy and IoT exposure has increased the attack surface area the region.

According to CFR, there are seven distinct types of state-sponsored cyber attacks based on their goals and techniques.

- *Data Destruction* involves cyber operations aimed at permanently deleting, corrupting, or rendering data unusable. Attackers may target critical databases, intellectual property, or operational systems to cause disruption or inflict economic and strategic damage.
- *Defacement* attacks refer to when threat actors alter the visual appearance or content of websites, often to spread propaganda, political messages, or undermine the credibility of the targeted organisation. These attacks are typically low in sophistication but high in symbolic impact.

- *Denial of Service (DoS)* and Distributed Denial of Service (DDoS) attacks flood a network or server with overwhelming traffic, rendering it inaccessible to legitimate users. Such attacks aim to disrupt services, cripple communications, and cause reputational or operational damage.
- *Doxing* refers to the unauthorized gathering and public release of sensitive personal information, often to intimidate, embarrass, or pressure individuals or organizations. State-linked doxing campaigns can target government officials, journalists, or dissidents.
- *Espionage* operations involve the clandestine theft of sensitive or classified information from governments, corporations, or individuals. These campaigns are often long-term and focus on strategic intelligence gathering, influencing foreign policy or gaining economic advantages.
- *Financial Theft* targets financial institutions, cryptocurrency platforms, or large corporations to steal funds directly or launder money. North Korean groups like *Lazarus* have been prominent in state-sponsored cyber financial theft operations.[10]
- *Cyber Sabotage* involves the deliberate disruption or degradation of physical, and usually critical, systems through cyber means. This can include attacks on industrial control systems, energy grids, or transportation infrastructure. *Stuxnet*, which targeted Iranian nuclear facilities, is a prime example of cyber sabotage.[11]

The data on cyber incidents in Southeast Asia illustrates an alarming trend. Between 2018 and 2025, the frequency of politically-motivated cyber operations targeting Southeast Asian states has escalated significantly (Figure 1). There's a clear uptick in incidents starting from 2018, peaking around 2022–2023. This indicates a persistent and escalated targeting of SEA nations, coinciding with broader geopolitical tensions and digitalization in the region.

Hacktivist groups, who often operate in alignment with nationalist agendas, have taken centre stage in these campaigns. For instance, amidst the armed conflict between Thailand and Cambodia, the Cambodian hacktivist group, AnonSecKh (also known as ANON-KH or Bl4ckCyb3r), claimed responsibility for 73 distributed denial-of-service (DDoS) attacks targeting Thai government bodies, military institutions, and key private sectors within a span of two weeks in July 2025.[12] Later, Nation Group, a Thai media conglomerate, announced that it has come under severe cyberattack originating from Cambodian users, which registered 223 million DDoS hits on its website and Facebook page within just 24 hours.[13] The level of coordination and the volume of the attack indicated not only technical

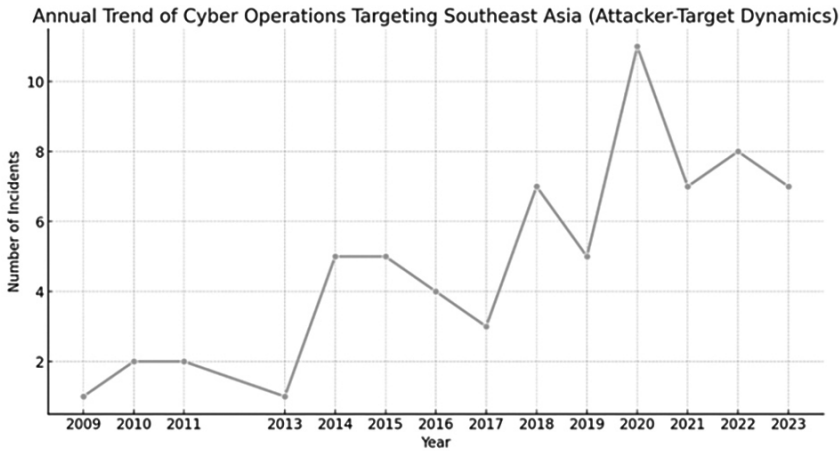


*Figure 1: Number of Incidents of Cyber Operations with Southeast Asian Nations as a Target*

Note: The slight dip in 2024 may reflect reporting lag or shifts in operational stealth, not necessarily a decrease in activity. Source: Surachanee 'Hammerli' Sriyai, based on data from the Council on Foreign Relations (CFR) Cyber Operations Tracker (2025).

capacity, but also a strategic intent to inflict operational disruption on a national scale.

Conversely, Thai hacktivist groups, such as BlackEye-Thai, have allegedly engaged in retaliatory operations against Cambodian governmental digital assets, compromising critical databases and leaking sensitive data.[14] These tit-for-tat cyber campaigns, exacerbated by the lack of effective conflict resolution mechanisms, have entrenched a cycle of escalation. Notably, groups like KH Night Mare have further amplified these hostilities by leaking up to 800GB of exfiltrated data in recent incidents, claiming to have breached Cambodia's top-secret servers.[15] These developments underscore the fluidity of attacker-target dynamics within the region, where nationalistic fervour and geopolitical grievances often manifest in cyberspace.

External actors also play a pivotal role in shaping the cyber threat landscape in Southeast Asia. State-sponsored threat actors from China, India, and Iran have been implicated in cyber espionage campaigns aimed at extracting intelligence from Southeast Asian governments and critical infrastructure sectors. These operations, often executed through sophisti-

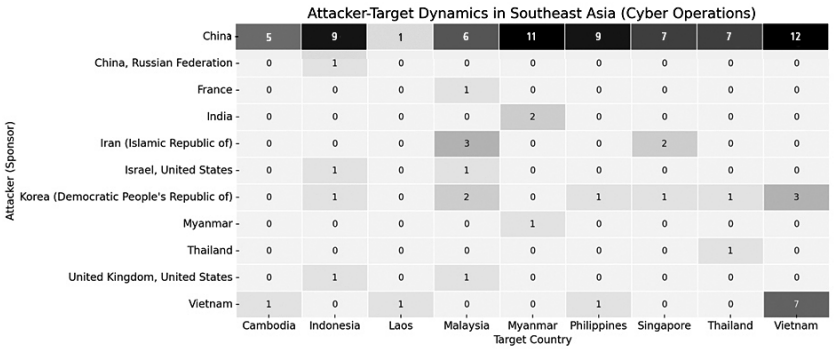


*Figure 2: Attacker-Target Dynamics Heatmap. Source: Surachanee 'Hammerli' Sriyai, based on data from the Council on Foreign Relations (CFR) Cyber Operations Tracker (2025).*

cated Advanced Persistent Threats (APTs), leverage obfuscation techniques such as botnets, proxy servers, and false-flag operations to mask their origins. This strategic ambiguity enables states to reap the benefits of cyber operations while maintaining plausible deniability, complicating efforts to establish accountability under international law.

An examination of incident trends reveals that Southeast Asia's cyber threat environment is not only intensifying but also evolving in its nature. From 2018 onwards, there has been a discernible uptick in cyber incidents, with a pronounced escalation during periods of heightened geopolitical tensions. The peak observed between 2022 and 2023 correlates with tensions in the South China Sea, the Ukraine war, domestic political upheavals in Thailand, and the overall growing entanglement of cyberspace in statecraft.[16] This pattern reflects a strategic shift where cyber operations have become an extension of geopolitical manoeuvring, allowing states and their proxies to project influence, conduct espionage, and undermine adversarial stability without crossing the threshold of kinetic conflict.

Figure 2 (above) presents an Attacker-Target Dynamics Heatmap, summarizing cyber operations in Southeast Asia.

Unsurprisingly, China has consistently established itself as the most persistent and widespread cyber threat actor targeting multiple countries within Southeast Asia. The primary objective of China's cyber operations in the region revolves around espionage with a clear focus on acquiring sensitive information from government bodies, defence institutions, and critical infrastructure sectors. Nations such as Thailand, Malaysia, Indone-

sia, and Vietnam frequently find themselves at the receiving end of Chinese-sponsored campaigns. These operations are typically sophisticated, prolonged, and multifaceted, reflecting Beijing's broader geopolitical ambitions to bolster its strategic leverage in Southeast Asia while maintaining a robust intelligence advantage.

In contrast, India's cyber operations in the region appear more narrowly focused on reconnaissance. APT groups linked to India, such as SideWinder, have been observed conducting espionage activities against countries like Thailand, Vietnam, and the Philippines on top of the usual South Asian government targets.[17] These operations largely concentrate on defence establishments and intelligence apparatuses, reflecting New Delhi's intent to gather actionable intelligence amidst ongoing geopolitical tensions in the region. Unlike China's broad spectrum cyber targeting that spans governmental and private sectors, India's cyber efforts are more concentrated on state-level targets, seeking specific strategic advantages.

Notably, Vietnam occupies a unique position in the region's cyber conflict landscape, as it operates both as a frequent victim and an active attacker. Vietnam-linked actors, often suspected to be state-sponsored proxies, have utilized cyber operations, such as DDoS attacks against political dissidents and opposition groups. These domestic campaigns signal an entrenched strategy of state-endorsed digital repression aimed at silencing dissent and consolidating political control over the information domain.[18] Vietnam's dual role illustrates how cyber tools are being repurposed not only for interstate conflicts, but also for domestic political surveillance and suppression.

Beyond the immediate regional neighbours, foreign actors like Iran have also made incursions into Southeast Asian cyberspace. Iranian cyber operations, while primarily orchestrated as part of larger, multi-region campaigns, have occasionally pursued Southeast Asian targets. These activities, often centred on mass espionage and disruptive cyber operations, exploiting regional cybersecurity vulnerabilities rather than treating the region as an intended target or pursuing Southeast Asia-specific strategic objectives. Iran's presence in the region underscores the broader reach of state-sponsored cyber actors who leverage global digital weaknesses to amplify their strategic campaigns. Additionally, Southeast Asia frequently becomes an unintended collateral battlefield in global cyber conflicts orchestrated by non-regional powers. The Stuxnet campaign, widely attributed to the joint operation between Israeli and US cyber forces, provides a prominent example where Southeast Asian systems, particularly in Indonesia, were

inadvertently drawn into a conflict that was primarily aimed at Iran's nuclear infrastructure. Such incidents highlight the transnational interconnectedness of cyberspace, where the porous boundaries of digital networks often entangle Southeast Asian entities in conflicts far removed from their own geopolitical interests. This collateral involvement exposes the region to unintended disruptions and emphasizes the global ripple effects of high-profile cyber warfare.

*Table 1: Comparison of Key Attacks, by Region*

| Key Dynamics | Southeast Asia | Europe | North America | Middle East | Latin America & Africa |
|---|---|---|---|---|---|
| State-Sponsored Espionage | High | High | High | High | Low to Moderate |
| Proxy/Hacktivist Operations | High | Moderate | Low, but impactful | Moderate | Low |
| Critical Infrastructure Targeting | Moderate with low repercussions | Moderate on High-value targets, but strong defence | Moderate, but robustly defended | High, often escalating to sabotage | Low |

Note: High ≥ 30 incidents; Moderate 10–29 incidents; Low < 10 incidents. Source: Surachanee 'Hammerli' Sriyai, based on data from the Council on Foreign Relations (CFR) Cyber Operations Tracker (2025).

In comparison to other regions, Southeast Asia's cybersecurity posture is markedly fragile as shown in Table 1 above. The radar chart positions Southeast Asia as a region facing persistent and strategically significant cyber threats, albeit with a narrower attacker ecosystem and attack type diversity compared to more cyber-saturated regions like North America and Europe. Unlike its Western counterparts that have been contending with a constant barrage of high-volume, multi-vector attacks from a wide array of threat actors ranging from nation-states, cybercriminal syndicates, to hacktivist groups, Southeast Asia's cyber threat landscape is dominated by a few key adversaries, notably China, with additional threats from India-linked groups and Iranian actors.

In North America, cyber operations are deeply entrenched in strategic competition, with the United States frequently targeted by APTs from Russia, China, Iran, and North Korea. The scale and complexity of attacks are

far more diverse and sophisticated. Similarly, Europe faces relentless cyber activity, particularly from Russian and Chinese APTs engaging in cyber-espionage, disinformation campaigns, and infrastructure attacks. However, unlike Southeast Asia, Europe has established more mature cyber defence mechanisms, including collaborative cybersecurity initiatives under EU frameworks and NATO's cyber defence structures. While Southeast Asia often struggles with fragmented, bilateral, or informal cyber cooperation, Europe benefits from binding commitments and well-resourced joint response capabilities.

The Middle East, while similar to Southeast Asia in terms of having a concentrated set of active cyber adversaries, differs in the intensity and strategic aggressiveness of operations. Cyber conflicts between Iran, Israel, and Gulf States frequently involve high-impact sabotage and espionage efforts. Like Southeast Asia, the Middle East also faces the challenge of cyber proxy warfare. However, cyber operations in Southeast Asia are more geared towards long-term strategic espionage, with comparatively fewer instances of outright sabotage or destructive attacks. Latin America, finally, remains the least impacted region in this comparison. The cyber threat landscape there is predominantly opportunistic, driven by financially motivated cybercriminals rather than sophisticated state-backed campaigns.

In essence, Southeast Asia is not yet a high-frequency cyber conflict zone like North America or Europe, but its strategic significance ensures it remains persistently targeted, particularly for espionage and information operations. Unlike the Middle East, where cyber operations are more openly aggressive and destructive, Southeast Asia's cyber battles are subtler but no less impactful, with a focus on long-term strategic gains rather than immediate sabotage. The region's lack of cohesive cyber defence frameworks, coupled with rising tensions among neighbouring states like Thailand and Cambodia, amplifies the risks of escalation.

Apart from what is indicated in the data, the region is also seeing rising volumes of business-email-compromise, cryptojacking, online scams and data-interception campaigns; in part because many Southeast Asian states have yet to fully harmonise their legislative regimes, forensic capabilities or inter-agency coordination mechanisms.[19] Meanwhile, capability gaps are also large: some states, like Singapore, have mature national CERTs and public-private collaboration, whereas others are still building from the ground up. This disparity means that attackers will often target the weakest link not merely within a country but across the regional supply chain. The academic work on ASEAN region-wide CERT coordination underscores

that, while ASEAN's initiative is promising, disparities in capability among member states persist. Moreover, interstate cooperation is challenged by differing legal frameworks, cross-border investigative constraints, and trust deficits between actors.[20] Thus, the variation matters: the nature of the threat (financial fraud vs. espionage), the sector of vulnerability (digital economy vs. critical infrastructure), and the partnering state's own capacity all differ. Therefore, any external cooperation must adapt to those differences rather than assume uniform baseline conditions or single-path solutions.

### *4.3.3. Implications for International Cooperation*

Because of the variation across the region, international cooperation in cybersecurity must satisfy several criteria:

- It must be *differentiated*: high-capacity hubs will benefit from intelligence fusion, threat-sharing and joint exercises; lower-capacity states need assistance building legal frameworks, forensic labs, and public-private communication channels.
- It must be *multi-dimensional*: technical assistance alone is insufficient. Cooperation must involve law enforcement, judicial mechanisms (mutual legal assistance, asset-recovery), public-private collaboration (industry telemetry sharing), and diplomatic dialogue (norms, supply chain resilience).
- It must emphasize *regionality and network effects*: because transnational cybercrime flows through multiple jurisdictions, strengthening region-wide platforms (sharing between ASEAN states, multi-state workshops) amplifies impact more than isolated bilateral deals.
- It must be *sustainable*: capacity building needs long-term investment, not one-off events. Tools, processes, and institutional memory must be built from the ground up, and not just take the form of ad hoc responses.

These implications point to how EU partners, including Germany, should frame their engagement: not merely concerned with the export of capability, but rather establishing partnerships aligned with the uneven landscape in Southeast Asia.

### 4.3.4. Recommendations for EU Countries

At the EU level, the bloc should integrate cybersecurity cooperation with Southeast Asia into its broader Indopacific strategy. This means dedicating budget lines for regional CERT reinforcement, capacity-building grants, joint forensic labs and shared private-sector-telemetry frameworks. An EU-wide initiative could fund a regional cybercrime forensics hub that offers shared services (digital evidence handling, financial-crime analytics) to smaller ASEAN states while countries with strong expertise in cybersecurity, such as Estonia, can contribute to capacity building efforts in the region. Furthermore, the EU should scale up public-to-private sector cooperation, encouraging European companies to share anonymised telemetry under legal safeguards, helping build situational awareness of regional trends.

For Germany in particular, the following concrete steps are proposed:

1. Launch a "German-ASEAN Cyber Capacity Facility": German development agencies (BMZ/GIZ) together with the German Federal Office for Information Security (BSI) should create a pooled funding and assistance mechanism to deploy mentors, incident-response teams, open-source forensic labs and legal-framework advisory services across ASEAN states.
2. Sponsor regional drills and shared tooling: Germany should fund and co-host with ASEAN partners annual live-fire or tabletop cyber-exercises, bringing together public, private and third-party actors. The drills should include cross-border incident simulation, multi-jurisdiction evidence-chain testing, and private-telemetry sharing.
3. Strengthen law enforcement and judicial cooperation: Germany should second prosecutors and forensic experts into regional teams (e.g., INTERPOL's cybercrime programmes) and establish fast-track protocols for mutual legal assistance (MLA), asset recovery, money-laundering tracing and victim-support for scam-networks. It can also be integrated with the multi-cluster initiative in Thailand, which is spearheaded by UNODC, to coordinate anti-crime efforts among state agencies in Southeast Asia in order to prevent and mitigate threats; especially in the aspect of scam operations.[21]
4. Promote research, standards and industry linkages: Germany should fund Southeast scholars, expert think tankers, and civil society to do research focusing on a broad range of cybersecurity and digital resilience

topics, such as baseline institutional capacity of national CERT, secure cloud/IoT practices, AI-driven cybercrime tactics and supply chain assurance.

In conclusion, Southeast Asia presents a rich but challenging cyber-security landscape. The region's digital economy growth, diverse legal and institutional capacities, and the varied threat-profiles of states mean that cooperation cannot be generic. For the EU and Germany, the path forward lies in *tailored, sustained, multi-stakeholder engagement*, blending diplomacy, development assistance, law enforcement cooperation and private-sector partnerships. Germany's existing technical and institutional firepower positions it well to become a leading partner for Southeast Asia in the cyber domain – provided it aligns its initiatives to the varied capacities and needs of the region rather than offering a one-size-fits-all solution.

## *Notes*

1 United Nations Office on Drugs and Crime (UNODC), *United Nations Convention against Cybercrime* (Vienna: UNODC, 2025).
2 Global Anti-Scam Alliance, *Global Scams on the Rise: Over Half of Adults Worldwide Report Scam Encounters, 23 % Lost Money, Global State of Scams 2025 Report*, 2025, https://www.gasa.org/post/global-scams-on-the-rise-over-half-of-adults-worldwide-report-scam-; United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia* (Vienna: UNODC, 2025).
3 ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), "About Us," 2026, https://ajccbc.ncsa.or.th/about-us/ (accessed January 19, 2026).
4 Cybersecurity and Infrastructure Security Agency (CISA), "United States and Singapore Expand Cooperation on Cybersecurity," press release, 2021, https://www.cisa.gov/news-events/news/united-states-and-singapore-expand-cooperation-cybersecurity (accessed November 11, 2025).
5 "Việt Nam, US Sign Cooperation Agreement on Cybersecurity," Việt Nam News, November 14, 2024, https://vietnamnews.vn/society/1667051/viet-nam-us-sign-cooperation-agreement-on-cybersecurity.html (accessed November 11, 2025).
6 Abbey Gita-Carlos, "PH, US, Japan Vow Cooperation to Enhance Cyber, Digital Resilience," *Philippine News Agency*, October 19, 2024, https://www.pna.gov.ph/articles/1235913 (accessed November 11, 2025).
7 Council of Europe, "Octopus Project: Regional Workshop on Cybercrime and Electronic Evidence in Southeast Asia," 2024, https://www.coe.int/en/web/cybercrime/-/octopus-project-regional-workshop-on-cybercrime-and-electronic-evidence-in-southeast-asia-1 (accessed November 11, 2025).
8 Council of Europe, "Operation SECURE: Strengthening Cybersecurity in Asia and the South Pacific," 2025, https://www.coe.int/en/web/cybercrime/-/operation-secure-strengthening-cybersecurity-in-asia-and-the-south-pacific (accessed November 11, 2025).

9 Council on Foreign Relations, "Cyber Operations Tracker," *CFR Interactives*, 2025, https://www.cfr.org/cyber-operations/ (accessed August 10, 2025).
10 "The Lazarus Heist: How North Korea Almost Pulled Off a Billion-Dollar Hack," *BBC News*, June 20, 2021, https://www.bbc.com/news/stories-57520169 (accessed August 10, 2025).
11 "Stuxnet Worm 'Targeted High-Value Iranian Assets'," *BBC News,* September 23, 2010, https://www.bbc.com/news/technology-11388018 (accessed August 10, 2025).
12 Michael Hipolito, "Thai Organisations Face Surge in Cyberattacks after Border Clash," *Security Brief*, June 18, 2025, https://securitybrief.com.au/story/thai-organisations-face-surge-in-cyberattacks-after-border-clash (accessed August 10, 2025).
13 "Cross-Border Cyberattacks Surge as Thailand–Cambodia Tensions Escalate," *Cyber Defense*, July 29, 2025, https://cyberdefensewire.com/cross-border-cyberattacks-surge-as-thailand-cambodia-tensions-escalate/ (accessed August 10, 2025).
14 Cyber Defense, *Cross-Border Cyberattacks Surge as Thailand–Cambodia Tensions Escalate*.
15 BlackCat.News, "Bammmm!!! Hacker Thai ซื่อ KH Night Mare ปล่อย...," Facebook post, July 28, 2025, https://www.facebook.com/permalink.php?story_fbid=pfbid07PwCTMTaRkSBszNkEg3v72AbZb6PQfzoq6NRV3dG1uxrqyih3divA6n8qczntorCl&id=61578863603543&rdid=UWs8FavFHv8Z1RHW# (accessed August 10, 2025).
16 Surachanee 'Hammerli' Sriyai, "Analysis of Cyber Attacks in Southeast Asia: Strategic Dynamics, Policy Gaps, and Recommendations," *ISEAS Perspective* 2025/104, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2025-104-analysis-of-cyber-attacks-in-southeast-asia-strategic-dynamics-policy-gaps-and-recommendations-by-surachanee-hammerli-sriyai/.
17 Nate Nelson, "SideWinder APT Caught Spying on India's Neighbor Govts.," *Dark Reading*, May 22, 2025, https://www.darkreading.com/cyberattacks-data-breaches/sidewinder-apt-spying-indias-neighbor-govts (accessed August 10, 2025).
18 David Bak, Surachanee 'Hammerli' Sriyai, and S. Meserve, "Internet and State Repression: A Cross National Analysis of the Limits of Digital Constraint," *Journal of Human Rights* 17, no. 5 (2018): 642–659; Surachanee 'Hammerli' Sriyai, "How Means for Digital Repression in Southeast Asia Have Unfolded in Recent Times," *ISEAS Perspective* 2024/65, https://www.iseas.edu.sg/wp-content/uploads/2024/08/ISEAS_Perspective_2024_65.pdf.
19 Council of Europe, "*Octopus Project: Regional Workshop on Cybercrime and Electronic Evidence in Southeast Asia*."
20 Benjamin T. F. Lee, Alexandra Tan, and Mark Chen, "ASEAN Cybersecurity Cooperation Strategy: Combating Cyber Terrorism and Hackers Through CERT Coordination," *International Journal of Law and Public Policy* (IJLAPP) 7, no. 1 (2025): 20–30, https://doi.org/10.36079/LAMINTANG.IJLAPP-0701.788; Surachanee 'Hammerli' Sriyai, "The Thai-Cambodian War of Cyber Attrition: Implications for ASEAN," *Fulcrum*, August 21, 2025, https://fulcrum.sg/the-thai-cambodian-war-of-cyber-attrition-implications-for-asean/.
21 Surachanee 'Hammerli' Sriyai, "Borderland Scam Centres and Cyber Threats: Policy Considerations for Thailand," ISEAS Perspective 2025/60, https://doi.org/10.48048/ASI.2025.274566.