Cybersphere: Journal of Digital Security
ISSN *(Online)*: 3104-6819
Volume 1, Issue 1, April-June, 2025, Page 07-12

Review Article
Received: 03-05-2025| Accepted: 15-06-2025| Published: 25-06-2025

Cyber Threat Intelligence Sharing Among ASEAN Nations: Opportunities and Strategic Gaps

Lee Xiang*[1]

Abstract

As Southeast Asia experiences unprecedented digital transformation and escalating cyber threats, effective threat intelligence sharing has become a critical imperative for regional security. This paper examines the evolving landscape of cyber threat intelligence (CTI) collaboration among ASEAN member states, analyzing institutional frameworks, operational mechanisms, and persistent challenges. Drawing on current initiatives and geopolitical contexts, we identify significant opportunities presented by ASEAN's multilateral approach while highlighting strategic gaps in implementation, capability alignment, and trust-building. Our findings reveal that despite advanced coordination structures, disparities in cyber maturity, sovereignty concerns, and limited private sector integration hinder optimal intelligence exchange. We propose actionable recommendations for enhancing ASEAN's CTI ecosystem through standardized protocols, capability bridging, and institutionalized multistakeholder engagement to strengthen collective cyber resilience.

Keywords

ASEAN Cybersecurity, Threat Intelligence Sharing, Cyber Resilience, Regional Cooperation, Cyber Norms, Capacity Building, Public-Private Partnerships, Cyber Diplomacy

1Independent Scholar, China

INTRODUCTION

The Imperative for Regional Cyber Cooperation

Southeast Asia represents one of the world's most digitally dynamic yet vulnerable regions, with internet penetration reaching 80% and a digital economy projected to exceed $1 trillion by 2030 (ASEAN Secretariat, 2023). This rapid digitalization has attracted sophisticated cyber threats, including an 82% surge in cybercrime between 2021–2022 (INTERPOL, 2023) and a documented 20% increase in China-linked state-sponsored attacks (MITRE Engenuity, 2023). The cross-border nature of these threats—targeting critical infrastructure, financial systems, and government networks—demands coordinated defensive measures that transcend national boundaries.

The Association of Southeast Asian Nations (ASEAN) has recognized cybersecurity as a strategic priority within its political-security pillar, establishing multiple coordination frameworks since 2017. However, the effectiveness of these initiatives remains uneven across its ten member states, which exhibit stark disparities in cyber capabilities. Singapore leads with an ASEAN Digital Integration Index score of 80.70, while Myanmar trails at 30.11 (ASPI, 2024). This fragmentation creates exploitable seams for threat actors, making intelligence sharing not merely advantageous but essential for collective defense. This paper examines how ASEAN's institutional mechanisms for CTI exchange function in practice, identifies structural and operational gaps, and proposes pathways toward a more resilient intelligence-sharing ecosystem.

ASEAN's THREAT LANDSCAPE: COMPLEXITY AND URGENCY

Escalating and Evolving Threats

Southeast Asia faces a confluence of cyber threats that leverage the region's digital growth and geopolitical significance. Criminal syndicates exploit expanding attack surfaces, with financially motivated incidents (ransomware, banking trojans, e-commerce fraud) predominating. The ASEAN Desk investigation into malware targeting e-commerce platforms, leading to arrests in Indonesia, exemplifies this trend (INTERPOL,

Corresponding Author:

2023). Simultaneously, state-sponsored operations—particularly those attributed to Chinese advanced persistent threat (APT) groups—have compromised government servers across Thailand, Malaysia, Vietnam, Indonesia, Myanmar, and Cambodia between 2019–2022, exfiltrating sensitive communications (U.S. Department of State, 2022).

Critical infrastructure represents an increasingly attractive target. Datin Sarah Al Bakri Devadason, Malaysia's Permanent Representative to ASEAN, highlighted threats against air travel security systems and financial institutions, emphasizing that "the borderless nature of cyberspace" enables rapid threat propagation (Devadason, 2023). The convergence of criminal and geopolitical motives creates a complex risk environment where attacks on one member state inevitably create spillover risks for others.

Geopolitical Dimensions

ASEAN's strategic position has made it a focal point for great-power cyber competition. The South China Sea disputes, unresolved maritime boundaries, and economic rivalries create fertile ground for cyber espionage and disruption campaigns. Compounding this challenge is the varying alignment of member states with external powers: while some collaborate closely with U.S. or Japanese cyber initiatives, others maintain stronger ties with China (ASPI, 2024). These divergent relationships complicate consensus-building on attribution and response protocols when cross-border incidents occur.

EXISTING CTI SHARING MECHANISMS: ARCHITECTURE AND INITIATIVES

ASEAN has developed a multi-layered approach to threat intelligence coordination, combining policy frameworks, operational platforms, and capacity-building programs.

Policy and Governance Frameworks

- Cybersecurity Cooperation Strategy: This strategy establishes cyber norms implementation, critical infrastructure protection, and regional capacity building as core priorities. It mandates the creation of an ASEAN Regional Computer Emergency Response Team (CERT) to coordinate intelligence sharing between national CERTs (ASEAN Secretariat, 2021). Though not yet operational, this initiative represents ASEAN's most ambitious attempt at institutionalizing CTI exchange.
- ASEAN Cybercrime Operations Desk: Operated through INTERPOL since 2018, this platform provides investigative support, disseminates Cyber Activity Reports, and facilitates joint operations. Its successes include disrupting cryptojacking campaigns and e-commerce malware operations (INTERPOL, 2023).
- Cyber Norms Checklist: Championed by Malaysia and Singapore, this practical framework translates UN norms into actionable steps for implementing responsible state behavior in cyberspace, including intelligence sharing (ASEAN Ministerial Conference, 2024).

Technical Platforms and Operational Networks

- Malware Information Sharing Platform: Launched by the ASEAN Defense Ministers' Meeting Cybersecurity and Information Centre of Excellence (ACICE), this technical infrastructure enables real-time exchange of indicators of compromise (IOCs) and threat analytics (ACICE, 2023).
- Cybersecurity Resilience and Information Sharing Platform: Hosted by Malaysia's central bank, this platform facilitates threat data exchange specifically among financial institutions—a critical sector given ASEAN's integrated banking networks (Bank Negara Malaysia, 2022).
- ASEAN Cyber Defense Network: This network connects military cyber commands to address threats to national security infrastructure and distribute intelligence products (ASEAN Defense Ministers, 2021).

Key ASEAN CTI Sharing Platforms and Functions

Platform	Lead Agency/Sponsor	Primary Function	Stakeholders
ASEAN Desk	INTERPOL	Cybercrime intelligence & investigations	Law enforcement agencies
ACICE Malware Platform	Defense Ministries	Malware data exchange	National CERTs, defense agencies
Financial Resilience Platform	Central Bank of Malaysia	Financial sector threat intelligence	Banking regulators, financial institutions
ASEAN Cyber Defense Network	ASEAN Defense Ministers	Defense-critical CTI sharing	Military cyber units
ASEAN Cyber Capacity Programme	Singapore	Capacity building & exercise coordination	Civilian agencies, CERTs

Capacity Building Ecosystems

- ASEAN Cyber Capacity Programme: Singapore-funded since 2016, this initiative trains officials in technical analysis, policy development, and incident response. Its extension, the ASEAN-Singapore Cybersecurity Centre of Excellence, has trained hundreds of officials (Singapore MCI, 2023).
- ASEAN-Japan Cybersecurity Capacity Building Centre: Located in Thailand, this facility aims to develop over 700 cyber professionals through technical training aligned with ASEAN's strategic needs (Japan MOFA, 2023).
- ASEAN Cyber Shield: An annual offensive-defensive cyber exercise initiated in 2023 that simulates complex attack scenarios to enhance technical information sharing and coordinated response capabilities (ACICE, 2023).

Strategic Opportunities for Enhanced Collaboration

ASEAN's institutional diversity creates fertile ground for developing a uniquely Southeast Asian model of intelligence sharing. Several high-potential pathways exist:

Leveraging ASEAN's Multilateral Architecture

The region's extensive network of dialogue partnerships offers access to technical resources without over-reliance on any single power. Japan's capacity-building center ($2 million funding), U.S. support for INTERPOL's Cyber Capabilities & Capacity Development Project, and Australia's capacity-building programs demonstrate how external partners can enhance indigenous capabilities (Japan MOFA, 2023; U.S. Department of State, 2022). The ASEAN Charter's principles of consensus and non-interference—the "ASEAN way"—provide a trusted framework for gradually deepening cooperation while respecting sovereignty concerns (ASEAN Secretariat, 2023).

Harmonizing Cyber Norms Implementation

The Cyber Norms Checklist provides a roadmap for translating abstract principles into operational practices. By developing a "regional model of cyber norms maturity" with measurable benchmarks—covering infrastructure, legal frameworks, and policy implementation—ASEAN could create assessment tools that facilitate mutual trust (ASEAN Ministerial Conference, 2024). Singapore and Malaysia's leadership in this initiative demonstrates how advanced cyber nations can drive regional standardization.

Cross-Sectoral Integration Opportunities

The interconnected nature of critical infrastructure enables cross-sector intelligence synergies:

- Energy-Cyber Nexus: Climate vulnerabilities highlighted in ASEAN's environmental policies create impetus for protecting smart grids and energy infrastructure through shared threat intelligence (ASEAN Secretariat, 2023).
- Financial Sector Leadership: The resilience platform's success illustrates how sector-specific sharing models can pioneer advanced practices later adopted by other sectors. Its

incident simulation exercises provide templates for healthcare, transportation, and energy (Bank Negara Malaysia, 2022).
- Digital Economy Incentives: With e-commerce and digital payments expanding, businesses have vested interests in collaborative threat mitigation. Public-private information sharing centers modeled on Singapore's facilities could operationalize this convergence (Singapore CSA, 2023).

Persistent Gaps and Implementation Challenges

Despite robust frameworks, ASEAN's CTI sharing ecosystem faces structural and operational constraints.

Capability and Resource Disparities

The cyber maturity gap between Singapore/Malaysia and Cambodia/Laos/Myanmar creates asymmetric burdens. Advanced states hesitate to share sensitive intelligence with partners lacking secure handling capabilities, while resource-constrained nations struggle to contribute actionable data (ASPI, 2024). This imbalance undermines reciprocity—a foundational principle of sustainable intelligence partnerships. ACICE's monthly threat reports represent progress, but participation remains skewed toward more capable members.

Institutional and Cultural Barriers

- Transparency Deficit: Defense and intelligence agencies—critical stakeholders in national cyber defense—resist disclosing capabilities or threat intelligence due to institutional secrecy norms. As noted by ASPI analysts, these entities often "see cyber norms as constraints rather than mechanisms for stability" (ASPI, 2024).
- Fragmented Governance: Overlapping initiatives create coordination inefficiencies. The absence of the ASEAN Regional CERT—two years after its proposal—reflects institutional inertia (ASEAN Secretariat, 2023).
- Limited Private Sector Integration: Despite rhetoric about multistakeholder approaches, financial sector platforms remain an exception rather than a norm. Most sharing occurs between state agencies, excluding the technology companies that manage critical infrastructure and possess unique threat visibility (Singapore CSA, 2023).

Legal and Trust-Related Constraints

- Sovereignty Sensitivity: Non-interference principles hinder cross-border incident response and intrusive monitoring. Ambiguity persists regarding permissible assistance during significant cyber incidents affecting multiple states (UNODA, 2021).
- Inconsistent Legal Frameworks: Divergent data protection laws, cybercrime statutes, and surveillance regulations complicate evidence sharing and joint investigations. Extradition barriers remain for cybercriminals operating across ASEAN jurisdictions (INTERPOL, 2023).
- Attribution Hesitancy: Political sensitivities surrounding state-sponsored attacks—particularly those linked to major powers—discourage public attribution, impeding collective deterrence postures (U.S. Department of State, 2022).

Strategic Recommendations: Toward an Integrated CTI Ecosystem

Addressing ASEAN's intelligence-sharing gaps requires pragmatic, phased approaches that respect sovereignty while progressively enhancing integration.

Institutional and Process Reforms

- Establish the ASEAN Regional CERT with Tiered Participation: Allow members to engage at multiple classification levels based on capability. Initial focus should be on unclassified IOC sharing before progressing to sensitive threat analytics (ASEAN Secretariat, 2021).
- Develop a Cyber Trust Framework: Implement graduated confidence-building measures, beginning with joint tabletop exercises and progressing to shared sensor deployments at neutral sites. ACICE should publish anonymized regional threat landscape assessments quarterly (MITRE Engenuity, 2023).

- Create Sectoral Information Sharing Centers: Expand the financial sector model to healthcare, energy, and transportation sectors with standardized data formats and protected sharing channels (Bank Negara Malaysia, 2022).

Bridging Capability Gaps

- Tiered Capacity Building: Regional training centers should offer differentiated streams: foundational IOC analysis for less-resourced nations and advanced threat hunting for cyber-mature states (Japan MOFA, 2023).
- Rotational Staffing Programs: Embed cyber personnel from developing states within Singapore's Cyber Security Agency or Malaysia's National Cyber Security Centre for skills transfer (Singapore MCI, 2023).
- Shared Tool Licensing: Pool regional budgets for threat intelligence platforms through ASEAN-wide procurement agreements (ASPI, 2024).

Enhancing Multistakeholder Engagement

As ASPI's dialogue concluded, "governments cannot implement cyber norms alone" (ASPI, 2024). Effective CTI sharing requires institutionalizing non-state actor participation:

- Industry Threat Intelligence Councils: Establish quarterly briefings between CERTs and critical infrastructure operators to exchange tactical intelligence (Singapore CSA, 2023).
- Academic Cyber Fusion Cells: Universities should establish regional research consortiums to analyze long-term threat trends (ASEAN University Network, 2023).
- Civil Society Liaison Roles: Create cybersecurity advisory panels including digital rights groups to ensure intelligence-sharing mechanisms incorporate privacy safeguards (UNODA, 2021).

Diplomatic and Normative Measures

- Adopt a Regional Cyber Incident Taxonomy: Develop ASEAN-specific classification standards for cross-border incidents to streamline reporting and response coordination (ASEAN Ministerial Conference, 2024).
- Pilot a Cyber Peacekeeping Framework: Deploy joint technical teams during national elections or major events in vulnerable member states (ACICE, 2023).
- Advance Cyber Diplomacy Coordination: Align positions on international cyber governance through pre-consultation before UN sessions, presenting unified ASEAN statements (UNODA, 2021).

CONCLUSION: REALIZING THE ASEAN CYBER COMMUNITY VISION

Cyber threat intelligence sharing represents both a technical imperative and a political test for ASEAN's community-building aspirations. While significant progress has occurred since 2017—particularly in institutional architecture creation—operational effectiveness remains hampered by fragmentation, distrust, and uneven capabilities. The region's complex geopolitics, far from being an insurmountable barrier, actually necessitates indigenous solutions that leverage ASEAN's unique convening power.

The path forward requires pragmatic incrementalism: focusing initially on non-controversial domains like financial sector threats and criminal malware tracking while gradually expanding into more sensitive areas. Singapore and Malaysia must continue providing leadership, but Thailand, Vietnam, and Indonesia should assume greater initiative to avoid bifurcated participation. Critically, ASEAN must resist merely replicating Euro-Atlantic intelligence models, instead developing approaches that reflect its consensus traditions and diversity.

The stakes extend beyond cybersecurity. Effective CTI sharing serves as a confidence-building measure that can spill over into other security domains. As ASEAN implements its Cybersecurity Cooperation Strategy toward the 2025 horizon, threat intelligence collaboration will prove decisive in determining whether the

region emerges as a coherent actor in cyberspace or remains a patchwork of vulnerable digital economies. By closing implementation gaps through institutional innovation, capability equalization, and inclusive governance, ASEAN can transform its collective vulnerabilities into shared resilience—establishing a distinctive model for the Global South.

REFERENCES

ACICE. (2023). *Malware Information Sharing Platform Launch Report*. ASEAN Defence Ministers' Meeting.

ASEAN Ministerial Conference on Cybersecurity. (2024). *ASEAN Cyber Norms Implementation Checklist*.

ASEAN Secretariat. (2021). *ASEAN Cybersecurity Cooperation Strategy 2021–2025*.

ASEAN Secretariat. (2023). *Digital Integration Index Report*.

ASPI (Australian Strategic Policy Institute). (2024). *Cyber Maturity in the ASEAN Region*.

Bank Negara Malaysia. (2022). *Cybersecurity Resilience and Information Sharing Platform Annual Review*.

Devadason, Sarah Al Bakri. (2023). Keynote address at ASEAN Regional Forum on Cybersecurity.

INTERPOL. (2023). *ASEAN Desk Cyber Activity Report 2022-2023*.

Japan Ministry of Foreign Affairs. (2023). *ASEAN-Japan Cybersecurity Capacity Building Centre Progress Report*.

MITRE Engenuity. (2023). *ASEAN Threat Landscape Assessment*.

Singapore Cyber Security Agency. (2023). *Public-Private Partnership Framework for CTI Sharing*.

Singapore Ministry of Communications and Information. (2023). *ASEAN-Singapore Cybersecurity Centre of Excellence Annual Report*.

U.S. Department of State. (2022). *Fact Sheet: Cyber Threats in Southeast Asia*.

UN Office for Disarmament Affairs. (2021). *Report on Cybersecurity Norms Implementation*.

Conflict of Interest: No Conflict of Interest

Source of Funding: Author(s) Funded the Research

How to Cite: Xiang , L (2025). Cyber Threat Intelligence Sharing Among ASEAN Nations: Opportunities and Strategic Gaps. *Cybersphere: Journal of Digital Security, 1*(1), 7-12.