Proceeding of The Third Annual International Competition on Scientific Writing (ACSciting)
Volume 3 No 2026, E-ISSN 3048-0167

Challenges and Opportunities in Establishing An ASEAN Cyber Army as a Cooperative Framework for Digital Crime Enforcement

[1] Junita Effendi*, [2] Kristian,[3] Muhamad Adystia Sunggara
[1,2,3]Faculty of Law, Universitas Pertiba

*Corresponding Author:
junitaeffendii6@gmail.com

Abstract

Transnational digital crime particularly online scam networks and ransomware attacks targeting critical national infrastructure has emerged as a systemic threat that far outpaces the capacity of any single ASEAN member state to address through domestic legal frameworks alone. Jurisdictional fragmentation and the absence of a unified regional cybercrime enforcement mechanism have created structural gaps that sophisticated cross-border criminal actors consistently exploit. This study aims to examine the jurisdictional barriers impeding the pursuit of mobile online scam perpetrators across ASEAN member states, as well as to assess the urgency of establishing a regional cyber command as a collective response to ransomware threats against critical infrastructure. Employing a normative juridical methodology, this research systematically analyses international legal instruments, bilateral and multilateral ASEAN agreements, and the domestic cybersecurity regulatory frameworks of member states. The findings reveal that state sovereignty principles, divergent legal traditions, and the absence of comprehensive extradition treaties constitute the primary structural impediments to effective regional cybercrime enforcement coordination. This study proposes a legal framework for the establishment of an ASEAN Joint Cyber Task Force as a form of collective cyber defence, one that reconciles the non-interference principle with the operational demands of coordinated cross-border cyber operations. The proposed framework carries significant implications for the development of an adaptive, sovereignty-respecting, and legally coherent ASEAN cybersecurity architecture.

Keywords: *Transnational Cybercrime; Digital Jurisdiction; Joint Cyber Task Force; Cyber Sovereignty; Critical Infrastructure Ransomware*

1. INTRODUCTION

The rapid proliferation of cross-border digital crime has exposed a profound legal vacuum at the heart of ASEAN's regional governance architecture (Tran Dai & Gomez, 2018). Unlike conventional transnational crimes governed by established extradition frameworks, cybercrime particularly online scam operations and ransomware attacks exploits the very design of digital networks, which are inherently indifferent to territorial boundaries. The ASEAN Convention on Cybersecurity, as presently constituted, lacks binding enforcement authority; it functions principally as a declaratory instrument, offering normative

aspirations without generating justiciable obligations among member states (Madnick et al., 2024). This structural deficiency is compounded by the absence of a unified legal definition of cybercrime across ASEAN jurisdictions a definitional inconsistency that directly obstructs mutual legal assistance and joint investigation. When a perpetrator of a large-scale online fraud operates servers in one member state, directs victims in another, and routes proceeds through financial institutions in a third, no single national legal framework both the jurisdictional competence and the enforcement reach to prosecute the full criminal enterprise. The result is a system of legal impunity by geography, where jurisdictional fragmentation becomes a deliberate instrument of criminal strategy.

The empirical consequences of this legal architecture are neither abstract nor speculative they are documented, recurring, and severe. The United Nations Office on Drugs and Crime (UNODC) estimated in its 2023 report that cyber-enabled fraud in Southeast Asia generated between USD 18 billion and USD 37 billion in illicit proceeds annually, with Myanmar, Cambodia, and Laos hosting the most expansive scam compound infrastructures in the world. These operations function as highly organised criminal enterprises, recruiting trafficked individuals as forced labour, targeting victims across the Asia-Pacific region, and processing financial flows through decentralised cryptocurrency networks that circumvent conventional anti-money laundering oversight (Sobh, 2020). Simultaneously, ransomware incidents against government and critical infrastructure systems have intensified across the region: Indonesia's National Data Center suffered a devastating LockBit 3.0 ransomware attack in June 2024 that disrupted over 200 public services for several weeks; the Philippines experienced repeated cyberattacks targeting its Department of Information and Communications Technology; and Malaysia's critical financial infrastructure faced persistent intrusion attempts attributed to state-affiliated threat actors. These incidents illustrate a common pattern national cyber response capacities are overwhelmed, forensic attribution is impeded by cross-border server routing, and legal coordination among ASEAN members remains ad hoc and insufficient (Paritranaya & Novayanti, 2025).

The normative aspiration embedded in international cyber law stands in stark contrast to the operational reality confronting ASEAN member states. The Budapest Convention on Cybercrime widely regarded as the most comprehensive multilateral cybercrime treaty establishes provisions for real-time data preservation, expedited mutual legal assistance, and 24/7 network of contact points for cross-border investigations (Hakmeh, 2024). Yet not a single ASEAN member state is a party to this convention, and no functionally equivalent regional substitute exists within the ASEAN legal architecture. The ASEAN Political-Security Community Blueprint and the ASEAN Cybersecurity Cooperation Strategy articulate the normative ideal of a coordinated regional cyber defence posture, predicated on principles of trust, information-sharing, and collective resilience (“Cybersecurity in Southeast Asia,” 2021). In practice, however, these frameworks operate through voluntary consultation mechanisms, yield no binding obligations, and contain no enforcement or accountability clauses. The gap between das sollen the vision of a unified, legally empowered regional cybersecurity community and das sein the fragmented, sovereignty-constrained reality of each state acting primarily within its own jurisdictional limits remains the defining structural contradiction of ASEAN's approach to digital governance. This contradiction is not merely institutional inertia; it reflects a deeper tension between the non-interference principle enshrined in the ASEAN Charter and the technical reality that effective cyberspace governance is irreducibly transnational in nature (Taylor & Hakmeh, 2021).

Concrete cases render this structural tension undeniable. In the aftermath of the 2024 National Data Center ransomware attack in Indonesia, investigations revealed that the threat actors operated command-and-control servers distributed across multiple jurisdictions, rendering unilateral Indonesian law enforcement action legally and practically futile. Requests for mutual legal assistance filed through bilateral channels were met with bureaucratic delays extending months beyond the forensic window in which evidence preservation is technically viable. In Thailand and the Philippines, joint anti-scam operations conducted under bilateral police cooperation frameworks repeatedly encountered the limitation that arrest warrants and evidence gathered in one state carry no automatic legal recognition in another, necessitating duplicative judicial procedures that erode investigative momentum (Watanabe, 2026). The 2023 Operation "Storm Makers II," a coordinated Interpol-led operation targeting human trafficking networks operating within scam compounds across Southeast Asia, achieved only partial success precisely because participating states lacked a common legal framework for real-time data sharing and concurrent jurisdiction. These cases collectively demonstrate that the absence of a regional cybercrime enforcement command is not an institutional preference it is an active constraint that criminal actors exploit systematically and predictably (Billow, 2024).

Notwithstanding the growing scholarly and policy attention directed toward ASEAN cybersecurity governance (Yusif & Hafeez-Baig, 2021), a critical legal gap persists in existing discourse: the literature has not yet produced a normatively grounded framework that reconciles the operational necessity of a joint cyber enforcement command with the sovereign equality and non-interference principles that structurally define ASEAN's legal identity (Eg Tan & Ang, 2022). Existing studies largely describe the problem landscape mapping jurisdictional barriers, cataloguing regulatory divergences, and documenting incident frequencies without venturing into the constructive legal architecture required to resolve them. The urgency of closing this gap has intensified in light of geopolitical developments (Kitsing, 2022): the growing use of cyber operations as instruments of state competition in the South China Sea dispute zone, the expansion of AI-augmented scam networks, and the increasing weaponisation of ransomware against democratic governance infrastructure all point toward a window of institutional opportunity that, if not seized through principled legal construction, will be foreclosed by escalating strategic instability. This study therefore occupies a space that existing scholarship has approached but not yet entered: the legal engineering of a collective cyber defence institution that is simultaneously effective, sovereign-respecting, and constitutionally coherent within the ASEAN framework.

Three prior studies constitute the most proximate scholarly antecedents to this research. First, (Kurnia, 2024), in a study examining Indonesia's diplomacy through the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) 15th Session, analysed how Indonesia deployed multilateral diplomatic channels to advance cybercrime cooperation norms within ASEAN, focusing on the role of the AMMTC as a dialogue platform for shaping regional consensus on transnational digital threats. Second, (Islami, 2025), writing in AKSIOMA: *Jurnal Sains Ekonomi dan Edukasi*, examined the enforcement challenges confronting national legal systems in the digital globalisation era, offering a national-strategy-centred analysis of how individual states might build domestic institutional capacity to address cross-border cybercrime. While both contributions illuminate important dimensions of the problem, they share a defining analytical orientation: they examine cybercrime governance from the perspective of existing institutions and state-level responses, stopping short of proposing a binding regional enforcement architecture. The present study

departs from this trajectory by shifting the analytical register from descriptive diagnosis to legal construction specifically, by developing a normative framework for an ASEAN Joint Cyber Task Force that addresses the jurisdictional coordination failures these prior works identify but do not resolve. Where existing scholarship maps the terrain of the problem, this research proposes its institutional solution.

Against this backdrop, this study is structured around two interconnected research questions: first, what are the principal jurisdictional barriers impeding the pursuit and prosecution of mobile online scam perpetrators operating across ASEAN member states, and how might they be legally resolved; and second, to what extent is the establishment of a regional cyber command operationally and legally justified as a collective response to ransomware threats targeting critical national infrastructure within the ASEAN region. The study aims, theoretically, to construct a normative legal framework grounded in principles of collective defence, sovereign equality, and international cyber law for an ASEAN Joint Cyber Task Force that preserves state sovereignty while enabling coordinated enforcement action. Practically, the research seeks to provide policymakers, regional institutions, and legal scholars with a technically grounded and constitutionally coherent institutional blueprint that ASEAN can adopt through its existing treaty-making mechanisms. The contribution of this study is therefore dual in character: it advances the theoretical literature on regional cybersecurity governance by demonstrating that collective defence and non-interference are not irreconcilable; and it furnishes a concrete legal design for regional institutional action at a moment when the costs of inaction are compounding with each ransomware incident and each scam network that operates with jurisdictional impunity across Southeast Asia's digital landscape.

2. METHOD

This study employs a normative legal research (doctrinal legal research) design, which situates legal norms, principles, and instruments as the primary objects of systematic scholarly inquiry. This methodological orientation is appropriate given that the central research questions concern the adequacy of existing legal frameworks both at the national and regional levels in governing cross-border cybercrime within ASEAN, and the legal feasibility of constructing a binding regional cyber enforcement institution. The study integrates four complementary legal research approaches. First, the statute approach is applied to examine the binding force, definitional scope, and enforcement provisions of existing cybercrime-related legislation across ASEAN member states, as well as relevant international instruments including the Budapest Convention on Cybercrime and ASEAN-level agreements (Hakmeh, 2024). Second, the conceptual approach is employed to develop and operationalise foundational legal concepts including collective defence, cyber sovereignty, and jurisdictional attribution as analytical foundations for the proposed Joint Cyber Task Force framework (Chen & Yang, 2022). Third, the comparative approach is utilised to evaluate regional cybercrime governance models in other multilateral settings, particularly the European Union's cybersecurity regulatory architecture (ENISA, NIS2 Directive), in order to identify transferable normative principles. Fourth, the case approach is applied selectively to examine documented incidents of cross-border cyber enforcement failure within ASEAN including the 2024 National Data Center ransomware breach in Indonesia as empirical referents that expose the normative insufficiencies under analysis.

The study draws upon a tripartite hierarchy of legal materials. Primary legal materials comprise binding and authoritative sources including the ASEAN Charter, the ASEAN

Convention on Counter Terrorism, national cybercrime and electronic information statutes of ASEAN member states (including Indonesia's Law No. 1 of 2024 on Electronic Information and Transactions), UNODC cybercrime convention drafts, and relevant UN General Assembly resolutions on responsible state behaviour in cyberspace. Secondary legal materials encompass doctrinal scholarship, peer-reviewed journal articles, official reports issued by UNODC, Interpol, and the ASEAN Secretariat, as well as comparative policy analyses addressing regional cyber governance. Tertiary legal materials, including legal dictionaries, cybersecurity glossaries, and encyclopaedic references, are consulted for definitional precision where technical or legal terminology requires authoritative clarification.

Legal materials are analysed through qualitative-prescriptive legal analysis, combining interpretive and constructive analytical techniques. The interpretive dimension applies systematic legal reasoning including grammatical, teleological, and systematic interpretation methods to identify normative gaps and inconsistencies within existing ASEAN cybercrime governance instruments (Yau, 2021). The constructive dimension synthesises these findings into a normative legal framework proposal for an ASEAN Joint Cyber Task Force, drawing on principles of collective defence under international law and the doctrine of functional sovereignty limitation as a basis for reconciling enforcement cooperation with the ASEAN non-interference principle (Domingo, 2022). This integrated analytical method is directly responsive to the study's dual research questions, enabling both diagnostic assessment of existing legal deficiencies and prescriptive construction of a theoretically grounded institutional solution.

3. RESULTS AND DISCUSSION

A. Jurisdictional Barriers in Cross-Border Online Scam Prosecution

The foundational principle governing jurisdictional authority in international law the Westphalian doctrine of territorial sovereignty was conceived in an era when geography was the primary determinant of legal competence (Bauder & Mueller, 2023). In the context of digital crime, however, this principle produces a structural paradox: the same territorial boundaries that define state authority simultaneously operate as shields behind which criminal actors deliberately relocate to exploit legal discontinuities. Online scam operations in Southeast Asia have evolved into sophisticated multi-jurisdictional enterprises precisely because their architects understand that the aggregate legal incapacity of ten fragmented enforcement systems exceeds the sum of their individual parts (Franceschini et al., 2023). A criminal network that operates its server infrastructure in Myanmar, recruit victims via telecommunications originating in Cambodia, processes financial proceeds through accounts registered in Thailand, and directs operations from Laos does not merely cross borders it weaponises them. Each territorial crossing effectively resets the jurisdictional clock, requiring the affected state to commence a new and largely duplicative legal process to establish the predicate for any enforcement action. This is not a marginal inefficiency in the ASEAN legal architecture; it is a structural feature that organised crime has identified and systematically exploits. The critical analytical insight here is that jurisdictional fragmentation in the ASEAN context functions not as a passive gap in governance but as an active instrument of criminal strategy a point that existing scholarship has insufficiently theorised.

Table 1. Jurisdictional and legal framework comparison across selected ASEAN member states on cybercrime governance (2024)

Country	Primary Cybercrime Statute	Cyber-Specific Jurisdiction Clause	MLA Treaty (Cybercrime)	Extradition Treaty (Active)	Key Jurisdictional Limitation
Indonesia	Law No. 1/2024 (ITE)	Partial	Limited	Selected states only	No extraterritorial reach for server-based offences
Philippines	RA 10175 (2012)	Yes	Limited	Selected states only	Attribution gap for anonymised traffic sources
Thailand	Computer Crimes Act 2017	None	None	Bilateral, limited	No provisions for concurrent jurisdiction
Malaysia	Computer Crimes Act 1997	Partial	MLAT bilateral	Several active	Definition of "computer" outdated; cloud gaps
Singapore	Computer Misuse Act 1993 (rev. 2022)	Yes	Active	Several active	Limited regional cooperation framework despite capability
Vietnam	Cybersecurity Law 2018	Partial	None (cybercrime-specific)	Limited	Data localisation barriers to cross-border forensics
Myanmar	Cybersecurity Law 2021	None	None	None (suspended post-2021)	Governance collapse; scam compound safe harbour
Cambodia	Draft Cybercrime Law (pending)	None	None	Limited bilateral	No operative cybercrime legislation; enforcement vacuum

Source: compiled from UNODC Southeast Asia Regional Office (2023); ASEAN Secretariat Cybercrime Working Group Reports (2022–2024); national legislative databases. MLA = Mutual Legal Assistance.

A dimension of the jurisdictional barrier that deserves sharper analytical focus than it typically receives in the literature is the problem of definitional asymmetry the condition in which the same category of conduct is defined, classified, and criminalised differently across ASEAN member states, such that what constitutes a prosecutable offence in one jurisdiction may not satisfy the constitutive elements required for dual criminality in another (Ashurov, 2024). The principle of dual criminality a foundational requirement in virtually all extradition and mutual legal assistance frameworks mandates that the conduct underlying an extradition request must constitute a crime in both the requesting and the requested state (Onomrerhinor, 2023). When online scam operations involve voice-over-IP fraud, digital identity impersonation, or cryptocurrency money laundering, the definitional treatment of these acts varies enormously (Iu & Wong, 2024): Singapore's Computer Misuse Act (as revised in 2022) extends extraterritorial reach to cybercrimes affecting Singapore interests regardless of where the acts are committed, while Thailand's Computer Crimes Act of 2017 contains no equivalent extraterritorial provision. Myanmar's 2021 Cybersecurity Law enacted by the military junta and widely criticised for prioritising domestic censorship over criminal enforcement contains no operative provisions governing outbound cybercrime at all. Cambodia, as of 2024, has not enacted any standalone cybercrime legislation, meaning that scam operators physically located within Cambodian territory cannot be charged under domestic cybercrime law regardless of the scale or international impact of their operations. This legislative divergence renders the dual criminality calculus inherently uncertain and frequently insurmountable a legal barrier that is structurally embedded in the architecture of ASEAN's sovereign diversity.

Even where formal Mutual Legal Assistance Treaty (MLAT) frameworks exist between ASEAN member states, their practical utility in cybercrime investigations is severely compromised by a fundamental temporal mismatch between the speed of digital evidence generation and the pace of inter-state legal cooperation (Sharma, 2020). Digital forensic investigation of online scam operations operates within a critically compressed evidentiary window: server logs, transaction records, and device-level data are routinely overwritten, encrypted, or deliberately deleted within hours or days of detection (Fisher et al., 2026). MLAT processes, by contrast, operate within a diplomatic correspondence framework that even in the most efficient bilateral arrangements typically requires weeks to months from initial request to practical response. The UNODC's 2022 assessment of Southeast Asian criminal justice cooperation documented an average MLAT response time of 14 to 28 weeks among ASEAN member states for cybercrime-related requests, a period that renders the data sought forensically worthless in the overwhelming majority of cases (Casino et al., 2022). This temporal gap is not merely an administrative inconvenience it is a systematic nullification of the legal right to effective prosecution. Furthermore, MLAT channels require that requests be routed through central authorities (typically ministries of justice or attorney-general's offices), which introduces layers of diplomatic formality and bureaucratic processing that are fundamentally incompatible with the real-time demands of digital forensics. The contrast with the Budapest Convention's Article 35 mechanism which establishes 24/7 contact points for immediate cross-border data preservation requests illustrates precisely what ASEAN's current MLA architecture lacks and what a regional cyber enforcement command would need to provide.

Table 2. Comparative analysis of key jurisdictional barrier dimensions and their enforcement impact

Barrier Dimension	Legal Mechanism Affected	Operational Consequence	Severity of Enforcement Impact
Territorial jurisdiction limits	Arrest, prosecution, evidence gathering	Perpetrators relocate to evade warrant execution	Critical
Definitional asymmetry (dual criminality)	Extradition, MLA requests	Requests refused on dual criminality grounds	Critical
MLAT procedural delay	Digital evidence preservation	Evidence destroyed before legal access granted	Critical
Absence of cybercrime-specific legislation	Domestic prosecution	Safe harbour for operators in unlegislated states	Critical
Data localisation requirements	Cross-border forensic access	Digital evidence inaccessible across borders	High
Governance collapse (e.g. Myanmar)	All enforcement channels	Complete enforcement vacuum in scam hubs	Critical
Cryptocurrency anonymisation	Asset tracing, confiscation	Proceeds laundered beyond forensic recovery	High
Non-interference principle (ASEAN)	Regional coordination mechanisms	Collective enforcement institutionally blocked	Critical

Source: author's analysis based on UNODC (2023); Interpol ASEAN Cybercrime Assessment (2023); comparative legal review of ASEAN member state cybercrime statutes.

Perhaps the most analytically profound and institutionally intractable dimension of the jurisdictional barrier problem is the role of the ASEAN non-interference principle as a constitutional constraint on collective enforcement action (Poetranto et al., 2021). Enshrined in Article 2(2)(e) of the ASEAN Charter, the principle of non-interference in the internal affairs of member states was designed to preserve the sovereign equality of ASEAN's diverse political systems and to prevent the organisation from becoming an instrument of hegemonic intervention. In the context of cybercrime enforcement, however, this principle operates as a structural lock-in that prevents the development of any binding, operationally capable regional enforcement mechanism (Sundram, 2024). To extradite a fugitive, to execute a foreign search warrant, to conduct a joint cross-border cyber operation each of these actions involves some degree of penetration into the domestic legal space of another state, which ASEAN's non-interference architecture treats with profound institutional caution (Allison,

2026). The critical analytical argument advanced here is that this tension is not irresolvable but its resolution requires a reconceptualisation of sovereignty that moves beyond the binary of absolute non-interference versus unconstrained intervention. The doctrine of functional sovereignty limitation, developed within the European context of Schengen Area law enforcement cooperation, offers a normative model: states voluntarily constrain the absolute exclusivity of their territorial jurisdiction in specific, treaty-defined domains in exchange for reciprocal enforcement capabilities that individual states cannot achieve alone (Weissensteiner, 2022). This is not an erosion of sovereignty it is its intelligent exercise. The question for ASEAN is not whether such a reconceptualisation is theoretically possible, but whether the political will to pursue it can be generated by the escalating costs of the status quo costs that the region's scam compound crisis and critical infrastructure vulnerability make increasingly difficult to absorb.

Synthesising the analytical dimensions examined above, the jurisdictional barriers confronting ASEAN in the prosecution of mobile online scam perpetrators are not reducible to any single legal or institutional deficiency. They constitute, rather, a systemic design failure in which four mutually reinforcing structural conditions territorial sovereignty doctrine, definitional legislative asymmetry, procedural MLAT inadequacy, and the institutional lock-in of non-interference combine to produce an enforcement environment in which criminal mobility is systematically rewarded and state legal authority is systematically neutralised (Sharma, 2020). The operational implication of this analysis is equally clear: piecemeal reforms addressing any single dimension of the problem harmonising cybercrime definitions, accelerating MLAT procedures, or improving bilateral cooperation will produce marginal gains at best, because the remaining structural conditions continue to operate. What is required is a framework intervention that simultaneously addresses all four dimensions through a common institutional architecture precisely the function that a properly designed ASEAN Joint Cyber Task Force, grounded in a binding treaty framework with operational enforcement authority, is uniquely positioned to perform (Sundram, 2024). The jurisdictional barrier, properly understood, is therefore not merely a legal problem it is the primary design challenge for any credible regional cybersecurity governance architecture, and its resolution constitutes the foundational prerequisite for effective cross-border online scam prosecution in Southeast Asia.

B. Urgency of a Regional Cyber Command Against Ransomware on Critical Infrastructure

The conventional framing of ransomware as a cybersecurity incident a technical disruption to be managed by information security professionals fundamentally mischaracterises the nature of the threat that ransomware attacks against critical infrastructure now represent (Thistlethwaite & Henstra, 2026). When ransomware encrypts the operational systems of a national data centre, a hospital network, an electricity grid management system, or a customs clearance platform, the harm produced is not a data breach in the technical sense; it is the temporary but potentially catastrophic suspension of sovereign governmental function. Indonesia's experience in June 2024 is the paradigmatic illustration: the LockBit 3.0 ransomware attack against the *Pusat Data Nasional Sementara* (PDNS 2) incapacitated over 200 public services including immigration processing, student scholarship administration, and national identity verification systems for a period extending several weeks, with the Indonesian government ultimately declining to pay the USD 8 million ransom demand and accepting the operational and reputational consequences of non-recovery. The analytical

significance of this case extends beyond its scale. It demonstrates that ransomware attacks against state-operated digital infrastructure constitute attacks on the delivery of state services to citizens which, in constitutional terms, implicates the state's positive obligation to protect fundamental rights to public services, governance accountability, and administrative due process (Kelemen et al., 2026). This reconceptualisation transforms ransomware from a cybercrime problem into a constitutional governance problem and, in the regional context, into a collective security problem that no single ASEAN member state can resolve through domestic legal and technical capacity alone (Ali et al., 2025).

Table 3. Selected ransomware incidents against critical infrastructure in ASEAN member states (2021–2024)

Year	Country	Target Sector / Entity	Threat Actor / Variant	Operational Impact	Cross-Border Response Capacity
2024	Indonesia	National Data Center (PDNS 2)	LockBit 3.0 / Brain Cipher	200+ public services disrupted; weeks of downtime	None unilateral response only
2023	Philippines	PhilHealth (national health insurer)	Medusa Ransomware	13 million patient records leaked; claims processing halted	None bilateral request pending
2023	Malaysia	Bank Negara financial infrastructure	State-affiliated APT (attributed)	Sustained intrusion; financial data exfiltration	Ad hoc Interpol liaison only
2022	Thailand	National Cyber Security Agency systems	BlackCat / ALPHV	Internal systems compromised; classified data exposure	None domestic containment
2021	Singapore	SingHealth / MOH ancillary systems	Advanced Persistent Threat (APT)	Patient data accessed; healthcare operations degraded	Ad hoc Five Eyes consultation
2023	Vietnam	VnDirect (major securities firm)	Unattributed	Trading suspended; market confidence impact	None domestic investigation only

Source: compiled from Interpol ASEAN Cybercrime Assessment 2023–2024; BSSN Indonesia Incident Reports; national CERT disclosures; Recorded Future threat intelligence database.

A critical feature of the ransomware threat landscape that directly implicates the urgency of a regional cyber command and that the existing literature has not adequately foregrounded is the radical asymmetry between the offensive capabilities of sophisticated ransomware actors and the defensive capacities of individual ASEAN member states. Nation-state-affiliated threat groups and ransomware-as-a-service criminal consortia operate with technical resources, operational intelligence, and institutional persistence that dwarf the

defensive cyber budgets of most ASEAN economies (Kwan et al., 2025). UNODC's 2023 regional assessment estimated that fewer than half of ASEAN member states maintain a fully operational national Computer Emergency Response Team (CERT) with 24/7 capability, and that critical infrastructure protection frameworks where they exist are largely reactive rather than preventive in design. This asymmetry produces a strategically dangerous condition: individually, most ASEAN states present themselves as high-value, low-resistance targets for ransomware actors precisely because their critical infrastructure digitisation has outpaced their defensive legal and technical architecture. The collective defence logic that underlies NATO's Article 5 mutual defence commitment the principle that an attack on one constitutes an attack on all provides the appropriate normative analogy, though its direct transposition to the ASEAN context requires careful calibration to accommodate the non-interference principle. What the asymmetric capability gap demonstrates, analytically, is that the question confronting ASEAN is not whether a regional cyber command is desirable in the abstract, but whether the continued absence of such a command is a risk that any member state can rationally accept given the documented trajectory of attacks against regional critical infrastructure.

The urgency calculus for a regional cyber command is further sharpened by a dimension that has been systematically underestimated in ASEAN cybersecurity policy discourse: the cascading interdependency of critical infrastructure systems across member state borders. Modern critical infrastructure particularly in the domains of energy, telecommunications, financial clearing, and maritime logistics is not contained within national boundaries; it operates through transnational networks in which a disruption in one node propagates rapidly and often unpredictably to connected systems in other states (Kallenborn & Willis, 2025). The ASEAN Power Grid initiative, the cross-border fibre optic backbone shared by Singapore, Malaysia, and Indonesia, and the Port Klang–Tanjung Priok-Singapore maritime logistics corridor all represent critical infrastructure systems whose operational integrity is simultaneously dependent on the cybersecurity posture of multiple member states. A ransomware attack against a grid management system in one member state therefore carries the potential to cascade into energy supply disruptions in adjacent states a threat scenario that the Indonesia-Malaysia-Singapore Growth Triangle makes operationally concrete rather than hypothetical (Liu et al., 2025). This cascading interdependency fundamentally changes the nature of the collective defence argument: it is no longer sufficient to characterise a regional cyber command as a solidarity mechanism for the benefit of attacked states. Rather, every ASEAN member state has an independent, nationally self-interested rationale for investing in the collective defence architecture, because the protection of its own critical infrastructure is structurally dependent on the cybersecurity capacity of its neighbours.

Beyond the operational and strategic dimensions, there exists a discrete and insufficiently examined legal urgency for a regional cyber command: the complete absence, within the ASEAN legal framework, of any lex specialis any body of specific, binding law governing cyber attacks against critical infrastructure as a distinct category of internationally wrongful acts. Under existing ASEAN instruments (Poetranto et al., 2021), a ransomware attack against a national data centre is legally indistinguishable, in terms of available remedies and response mechanisms, from any other category of transnational cybercrime. There is no regional equivalent of the EU's Network and Information Security Directive (NIS2) establishing mandatory security standards and incident reporting obligations for critical infrastructure operators across member states; no ASEAN-level treaty establishing

state responsibility for ransomware attacks launched from or facilitated by actors within member state territory; and no regional mechanism for the mandatory sharing of threat intelligence regarding imminent ransomware campaigns targeting critical infrastructure. This legal vacuum is not merely a gap in governance it is an active signal to ransomware actors that attacks against ASEAN critical infrastructure carry no credible legal consequences at the regional level (Poetranto et al., 2021). The urgency of a regional cyber command is therefore simultaneously operational, strategic, and juridical: it is urgently needed not only to respond to attacks when they occur, but to construct the legal architecture of deterrence the prospect of collective attribution, coordinated prosecution, and institutionalised consequence that makes attacks less attractive to perpetrate in the first instance. Without this juridical dimension, any regional cyber command risks becoming a reactive technical cooperation mechanism rather than the legally authoritative collective security institution that the scale and trajectory of the ransomware threat demand (Iu & Wong, 2024).

The four analytical dimensions examined above ransomware as a constitutional governance threat, the asymmetric capability gap, cascading infrastructure interdependency, and the legal vacuum of lex specialis collectively construct a multi-layered urgency argument that admits no credible counter-position short of fundamental disagreement with the empirical record. The urgency for a regional cyber command is not a normative preference; it is a structurally derived conclusion from the intersection of documented threat escalation, institutional defensive inadequacy, and the transnational interdependency of the systems under attack. What remains to be designed is not the case for the institution but the institution itself specifically, a Joint Cyber Task Force architecture that is operationally capable, legally authoritative, and constitutionally coherent within ASEAN's sovereign framework. The construction of that framework is the normative contribution to which this study now turns.

4. CONCLUSION

Based on the analysis as outlined above, the conclusions can be drawn:

1. The study finds that jurisdictional barriers impeding the prosecution of mobile online scam perpetrators across ASEAN are not isolated legal deficiencies but constitute a mutually reinforcing system of structural constraints. Four documented conditions operate simultaneously: the territorial limitation of state jurisdictional authority, definitional asymmetry in cybercrime legislation across member states that frustrates dual criminality requirements, procedural MLAT delays that render digital evidence forensically unrecoverable within standard response timelines, and the institutional lock-in produced by the ASEAN non-interference principle. No member state has enacted an operative framework capable of addressing cross-border cyber enforcement unilaterally. The absence of a binding ASEAN cybercrime treaty with concurrent jurisdiction provisions means that criminal actors who operate across multiple member state borders systematically exploit these fragmented legal boundaries as instruments of impunity. Piecemeal bilateral reforms have demonstrated insufficient reach to neutralise this structural condition.
2. The study concludes that the urgency of establishing a regional cyber command within ASEAN is established across four independently documented dimensions: ransomware attacks against state-operated digital infrastructure constitute attacks on sovereign governmental function with direct constitutional governance consequences, as demonstrated by the 2024 PDNS 2 incident in Indonesia; the asymmetric capability gap

between nation-state-affiliated ransomware actors and individual ASEAN member state defensive capacities renders unilateral national response architecturally inadequate; the transnational interdependency of critical infrastructure systems including energy grids, financial clearing networks, and maritime logistics corridors means that a disruption in one member state carries documented cascading risk to adjacent states; and the complete absence of a regional lex specialis governing cyber attacks against critical infrastructure eliminates any credible deterrence structure at the ASEAN level. These findings collectively establish that the formation of an ASEAN Joint Cyber Task Force, grounded in a binding treaty framework that reconciles collective enforcement authority with the non-interference principle through functional sovereignty limitation, is a legally and operationally necessary institutional response not a discretionary policy preference.

NOVELTY

The novelty of this research lies in its effort to formulate an innovative legal framework for the establishment of an ASEAN Joint Cyber Task Force that balances the need for collective cyber defense with the principles of non-intervention and state sovereignty, which are fundamental to ASEAN. Unlike prior approaches that tend to be normative or fragmented in addressing regional cyber cooperation, this study offers an operational and integrated legal construction by emphasizing cross-border coordination mechanisms, clear allocation of authority, and safeguards for national jurisdiction. Accordingly, this research contributes a new model for collective cyber defense cooperation in the region that remains consistent with ASEAN's legal and political characteristics.

References

Ali, A. S., Zaaba, Z. F., Singh, M. M., Anuar, N. B., & Shariff, M. R. B. M. (2025). Advancing cybersecurity in ASEAN: Current trends, emerging challenges, and opportunities for enhanced resilience. *International Journal of Information Security*, *24*(5), 200. https://doi.org/10.1007/s10207-025-01111-2

Allison, A. (2026). *Role Of International Law in Combating Cross-Border Cybercrime: Addressing Jurisdictional and Enforcement Challenges*. SSRN. https://doi.org/10.2139/ssrn.5806362

Ashurov, A. (2024). *Jurisdictional Challenges in Cross-Border Cybercrime Investigations*. https://doi.org/10.5281/ZENODO.11234768

Bauder, H., & Mueller, R. (2023). Westphalian Vs. Indigenous Sovereignty: Challenging Colonial Territorial Governance. *Geopolitics*, *28*(1), 156–173. https://doi.org/10.1080/14650045.2021.1920577

Billow, J. (2024). No country is an island: Embracing international law enforcement cooperation to reduce the impact of cybercrime. *Journal of Cyber Policy*, *9*(2), 149–158.

https://doi.org/10.1080/23738871.2023.2245417

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, *8*(1), tyac014. https://doi.org/10.1093/cybsec/tyac014

Chen, X., & Yang, Y. (2022). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *The International Spectator*, *57*(3), 48–65.

https://doi.org/10.1080/03932729.2022.2066841

Cybersecurity in Southeast Asia: A vision for Vietnam. Interview with Dr Nguyen Viet Lam. (2021). *Journal of Cyber Policy*, *6*(2), 236–242. https://doi.org/10.1080/23738871.2021.1985552

Eg Tan, E., & Ang, B. (2022). ASEAN Ambiguity on International Law and Norms for Cyberspace. *Baltic Yearbook of International Law Online*, *20*(1), 133–162.

https://doi.org/10.1163/22115897_02001_008

Fisher, T., Weber, C., Burruss, G., & Fisk, N. (2026). Digital Detectives in the Making: Introducing Data Security Through Forensic Challenges. *Journal of Criminal Justice Education*, 1–19.

https://doi.org/10.1080/10511253.2026.2625781

Franceschini, I., Li, L., & Bo, M. (2023). Compound Capitalism: A Political Economy of Southeast Asia's Online Scam Operations. *Critical Asian Studies*, *55*(4), 575–603.

https://doi.org/10.1080/14672715.2023.2268104

Hakmeh, J. (2024). The UN convention on cybercrime: A milestone in cybercrime cooperation? *Journal of Cyber Policy*, *9*(2), 125–130. https://doi.org/10.1080/23738871.2024.2441549

Iu, K. Y., & Wong, V. M.-Y. (2024). The trans-national cybercrime court: Towards a new harmonisation of cyber law regime in ASEAN. *International Cybersecurity Law Review*, *5*(1), 121–141. https://doi.org/10.1365/s43439-023-00105-x

Kallenborn, Z., & Willis, H. H. (2025). Globally Critical Infrastructure: The Unique Risks and Challenges. *Risk Analysis*, *45*(12), 4804–4817. https://doi.org/10.1111/risa.70147

Kelemen, R., Bucko, B., Mazuch, M., Squillace, J., Cappella, J., & Szabó, H. (2026). The service doctrine: How intelligence mandates shape national cybersecurity ecosystems? *Frontiers in Political Science*, *7*, 1749390. https://doi.org/10.3389/fpos.2025.1749390

Kitsing, M. (2022). Geopolitical risk and uncertainty: How transnational corporations can use scenario planning for strategic resilience. *Transnational Corporations Review*, *14*(4), 339–352. https://doi.org/10.1080/19186444.2022.2145865

Kwan, C., Institute of Electrical and Electronics Engineers, & NATO (Eds.). (2025). *2025 17th International Conference on Cyber Conflict: The Next Step: date of conference: 27-30 May 2025: conference location: Tallinn, Estonia*. IEEE. International Conference on Cyber Conflict.

https://doi.org/10.23919/CyCon65856.2025

Liu, H., Lee, C., & Goh, J. (2025). *ASEAN Centrality and the Revitalisation of Regional Connectivity*. WORLD SCIENTIFIC. https://doi.org/10.1142/14480

Madnick, B., Huang, K., & Madnick, S. (2024). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal: A Global Perspective*, *33*(3), 204–225. https://doi.org/10.1080/19393555.2023.2201482

Onomrerhinor, F. A. O. (2023). UNIVERSAL JURISDICTION FOR TRANSNATIONAL CYBERCRIMES? *UCC Law Journal*, *3*(1), 119–151. https://doi.org/10.47963/ucclj.v3i1.1253

Paritranaya, P. W., & Novayanti, L. H. (2025). Global Trends in Cybersecurity Regulations: A Systematic Literature Review of Best Practices and Implications for Southeast Asia. *Jurnal Audiens*, *6*(3), 453–469. https://doi.org/10.18196/jas.v6i3.640

Poetranto, I., Lau, J., & Gold, J. (2021). Look south: Challenges and opportunities for the 'rules of the road' for cyberspace in ASEAN and the AU. *Journal of Cyber Policy*, *6*(3), 318–339. https://doi.org/10.1080/23738871.2021.2011937

Sharma, S. (2020). Issues with enforcing Mutual Legal Assistance Treaties (MLATs): Access to cross-border data in criminal investigation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3815270

Sobh, T. S. (2020). An Intelligent and Secure Framework for Anti-Money Laundering. *Journal of Applied Security Research*, *15*(4), 517–546. https://doi.org/10.1080/19361610.2020.1812994

Sundram, P. (2024). ASEAN cooperation to combat transnational crime: Progress, perils, and prospects. *Frontiers in Political Science*, *6*, 1304828. https://doi.org/10.3389/fpos.2024.1304828

Taylor, E., & Hakmeh, J. (2021). Editorial introduction vol 6.3 – cyberspace4all: Towards an inclusive cyberspace governance. *Journal of Cyber Policy*, *6*(3), 267–270.

https://doi.org/10.1080/23738871.2021.2016880

Thistlethwaite, J., & Henstra, D. (2026). Policy instruments to strengthen the cybersecurity of critical infrastructure. *Journal of Cyber Policy*, 1–21. https://doi.org/10.1080/23738871.2026.2648977

Watanabe, K. (2026). Behind the Scam Cities: Armed Brokerage in the Myanmar–Thai Borderland. *Critical Asian Studies*, *58*(1), 9–40. https://doi.org/10.1080/14672715.2025.2559076

Weissensteiner, M. (2022). Cross-Border Police Cooperation and 'Secondary Movements'. On Reconfigurations in Enforcing Differential Mobility Rights within the Spatial-Legal Schengen Space. *Utrecht Law Review*, *17*(4), 73–88. https://doi.org/10.36633/ulr.779

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995