PUNGGAWA
LAW REVIEW
Punggawa Law Review
Volume 1, Number 1, 2026
E-ISSN: xxxx-xxxx
Open Access: punggawajournal.com/plr

From Territoriality to Functional Control: A Jurisdictional Test for Cross-Border Cyberterrorism Operations

Nadiah Khaeriah Kadir[1]
[1] Fakultas Hukum Universitas Hasanuddin, Indonesia
Correspondence: nadiahkhaeriah@unhas.ac.id

Article Info
Article history:
Received Feb 28, 2026
Revised Mar 1, 2026
Accepted Mar 4, 2026

Keyword:
Cyberterrorism; International jurisdiction; Extraterritorial jurisdiction; Sovereignty; Non-intervention.

ABSTRACT
Cyberterrorism repeatedly challenged jurisdictional reasoning because its conduct, infrastructure, effects, and evidence were distributed across multiple states, making territorial and effects-based claims both over-inclusive and operationally fragile. This article examined why classical jurisdiction bases produced recurring gaps and conflicts in cross-border cyberterrorism prosecutions and proposed a control-oriented solution. It developed a Functional Control Test that assessed jurisdictional priority by reference to operational direction, meaningful leverage over enabling infrastructure, deliberate targeting and foreseeable coercive effects, and the lawful feasibility of securing decisive electronic evidence. The analysis showed that the test reduced inflated claims driven by incidental routing or compromised nodes, while still accommodating legitimate concurrent jurisdiction for deliberately targeted victim states. It also clarified that strong jurisdiction to prescribe and adjudicate did not entail unilateral cross-border enforcement, preserving consistency with sovereignty and non-intervention constraints. The study concluded that functional control provided a more reviewable and practicable nexus standard for allocating prosecutorial leadership and structuring cooperation in cyberterrorism cases.

INTRODUCTION

Cyberterrorism has become a jurisdictional stress-test for international criminal law because the architecture of the offence is rarely coextensive with territory. A cross-border operation can be initiated from one state, orchestrated through compromised devices in dozens of others, routed via cloud infrastructure that shifts location dynamically, and produce harmful effects in still different jurisdictions (Ryngaert, 2023). In that setting, the familiar question "where did the crime occur" becomes less a geographic inquiry than a contest of narratives about which connection should count as legally decisive. The practical consequence is predictable. Some cases fall into enforcement paralysis when no state can assemble a coherent chain of evidence or custody without external cooperation (Abraha, 2021). Other cases trigger simultaneous, expansive claims grounded on diffuse "effects," generating overreach, duplicative prosecutions, or politicized extradition battles (Schmitt, 2021). Cyberterrorism thus exposes a structural mismatch between the territorial instincts of criminal jurisdiction and the functional reality of digital operations, where control and causation are distributed across layers of infrastructure and governance.

The doctrinal toolkit is not empty, but it is stretched. Territoriality, nationality, passive personality, and the protective principle can each be invoked, yet their application in the cyberterrorism context often turns on unstable proxies. "Server location" is a poor anchor when data is replicated across regions and execution is serverless (Eichensehr, 2022). "Effects" can be framed so broadly that almost any state with a victim or a downstream disruption can claim an objective territorial nexus, a move that risks converting jurisdiction into a security rhetoric rather than a disciplined legal judgment. Nationality-based jurisdiction presupposes reliable attribution and identification; cyberterrorism commonly defeats that assumption through anonymization, proxying, and the use of criminal

infrastructure markets. The protective principle appears attractive because cyberterrorism is frequently described as an attack on national security, yet that very elasticity makes it vulnerable to abuse: the looser the threshold of "threat," the easier it becomes to justify extraterritorial criminalization and to erode the distinction between legitimate counterterrorism and unilateral policing beyond borders. The result is not merely academic uncertainty. It is an operational problem that affects the legality of evidence acquisition, the fairness of proceedings, and the stability of inter-state relations.

This article addresses that mismatch by proposing a jurisdictional standard calibrated to the way cyberterrorism is actually executed and proven. The central claim is that jurisdiction in cross-border cyberterrorism should be anchored less in geography and more in demonstrable control over the functions that make the operation possible. The proposed approach, labelled a Functional Control Test, treats jurisdictional nexus as a question of whether a state is meaningfully connected to the operational direction of the attack, the leverage over the relevant infrastructure, the targeting and foreseeability of harmful effects, and the feasible reach over key evidentiary material through lawful channels (Rusdianto & Risnain, 2023). The point is not to replace the classic bases of jurisdiction as a matter of black-letter law, but to discipline their application by shifting the justificatory burden: rather than asserting territorial or protective claims at a high level of abstraction, states would be expected to show concrete, operation-linked control factors that explain why a particular forum is legitimate and why alternative forums are weaker.

The contribution is threefold. First, the article offers a structured diagnosis of why territoriality-centred reasoning produces both gaps and excess in cyberterrorism cases, especially where infrastructure is distributed, ownership is layered, and attribution is contested. Second, it formulates the Functional Control Test as a practicable nexus assessment that can guide jurisdiction to prescribe and adjudicate without collapsing into an endorsement of unilateral cross-border enforcement. That distinction matters (Beckerman, 2022). Even if a state has a strong basis to criminalize and prosecute, coercive investigative acts in another state's territory remain constrained by sovereignty, non-intervention, and the procedural architecture of cooperation. Third, the article demonstrates how the test operates across common operational patterns, including botnet-enabled attacks, cloud-based orchestration, and platform-mediated coordination, showing how the same control-oriented logic can reduce arbitrary forum selection while preserving space for concurrent jurisdiction where genuinely warranted.

Three research questions guide the analysis. What is the most persistent failure mode of territorial and effects-based jurisdiction when applied to cyberterrorism operations that are fragmented across infrastructure layers and jurisdictions? How can a control-oriented nexus test be articulated in a way that remains compatible with general international law principles, including sovereignty and non-intervention, while still responding to counterterrorism imperatives? And when applied to realistic cross-border scenarios, does the Functional Control Test generate outcomes that are more coherent, more predictable, and more defensible from the standpoint of due process and evidentiary integrity than the status quo?

The argument proceeds from a simple premise: cyberterrorism is operationally defined by control relationships that are often more legally salient than physical location. Control over command-and-control channels, administrative privileges, domain management, cloud identities, or the mechanisms that sustain an attack is not a metaphysical concept; it is the practical hinge on which both causation and proof turn (Abraha, 2021). A jurisdictional approach that foregrounds those control relationships offers a way to prioritize forums that can plausibly conduct lawful, effective, and fair proceedings, while discouraging expansive claims grounded only in diffuse downstream effects. In a field where enforcement power tempts legal shortcuts, the objective is to make jurisdictional reasoning more explicit, reviewable, and constrained by demonstrable operational facts rather than security intuition.

RESEARCH METHODS

This study employs normative (doctrinal) legal research, combining a conceptual approach to evaluate the adequacy of classical jurisdictional bases in cross-border cyberterrorism cases and to formulate the Functional Control framework as a structured method of jurisdictional reasoning. The legal materials consist of primary sources drawn from general international law principles relevant to jurisdiction and constraints on cross-border action (including sovereignty, non-intervention, and due

diligence), as well as key cooperation architectures for cross-border access to e-evidence, and secondary sources comprising recent peer-reviewed journal literature on extraterritorial jurisdiction, sovereignty in cyberspace, due diligence, and electronic evidence governance. Collection of legal materials is conducted through a systematic library-based review and targeted academic database searches, with sources selected based on direct relevance to jurisdictional nexus, enforcement limits, and evidentiary feasibility. Analysis is qualitative and argumentative, using doctrinal interpretation and legal reasoning to map where territoriality and effects-based claims become indeterminate in distributed cyber operations, and to assess the internal coherence and external fit of the Functional Control framework against international law constraints and the evidentiary requirements highlighted in the discussion.

RESULTS AND DISCUSSION

1. Why Territoriality Alone Fails: A Structural Diagnosis

Territoriality fails in cross-border cyberterrorism not because territory has become irrelevant, but because the operational architecture of cyber operations disaggregates the elements that territoriality assumes will travel together. Traditional territorial reasoning presumes a relatively stable alignment between conduct, actor, instrumentality, and evidentiary trace: an offender acts somewhere, using means that are situated somewhere, producing results somewhere, leaving proof that a forum can lawfully seize somewhere. Cyberterrorism breaks that alignment (Osula et al., 2022). It separates initiation from execution, execution from effects, and effects from the most probative evidence. Once those links are severed, territoriality becomes a partial descriptor rather than a reliable jurisdictional anchor, and the system oscillates between under-enforcement and over-assertion (Olber, 2021).

A first structural driver is the shift from localized infrastructure to layered, mobile computation. Cloud services, content delivery networks, virtualization, and serverless architectures are designed precisely to abstract computation away from fixed geography. Data is replicated, sharded, cached, and rerouted based on performance and resilience logic rather than territorial boundaries. As a result, the "location" of a cyberterrorism operation becomes a moving target. A prosecutor can point to a data center in the forum today, only for the same service to be served from a different region tomorrow. Even within a single incident, traffic may traverse or terminate in jurisdictions that are technically incidental to the operator's control decisions. Treating those incidental locations as dispositive territorial hooks is legally fragile and strategically perverse, because it rewards accidents of routing over the intentional architecture of the operation. It also creates incentives for offenders to "jurisdiction shop" defensively by selecting hosting arrangements that maximize fragmentation and exploit slow cooperation channels.

A second driver is the phenomenon of delegated presence created by botnets and compromised hosts. Many cyberterrorism operations rely on distributed networks of hijacked devices—home routers, IoT devices, servers, or even industrial systems—used as stepping-stones or as the attack surface itself. Territoriality is tempted to treat each infected node as a territorial manifestation of the offence, thereby multiplying territorial nexuses across dozens of states. Yet the node's location often has little to do with the operator's meaningful control other than the fact of compromise. The operator did not "enter" those territories in a conventional sense; the operator exploited vulnerabilities that existed there, and the devices acted as coerced intermediaries. If the mere presence of coerced intermediaries in a forum suffices to justify strong territorial jurisdiction, territoriality becomes over-inclusive and potentially arbitrary. More importantly, it confuses the locus of operational direction with the locus of instrumentalization, a distinction that matters both for culpability assessment and for legitimate forum selection (Nurkhasanah & Prasetyo, 2024).

A third driver is that the evidentiary heart of cyberterrorism is frequently extraterritorial to the primary victim state and sometimes extraterritorial even to the state where the operator physically sits. Modern cyber investigations hinge on technical artefacts that are created, retained, or controlled by intermediaries: authentication logs, cloud audit trails, platform metadata, payment records, domain registrars, and infrastructure monitoring data. Those artefacts are governed by corporate retention policies and by the domestic law of the jurisdiction that can compel the provider. This displaces the practical center of gravity from "where the harm was felt" to "where the evidence can be lawfully obtained." A territorial claim grounded in local effects may thus be weak if the forum cannot compel the relevant providers, cannot preserve volatile logs in time, or cannot establish a chain of custody accepted by its courts. Conversely, a state with minimal local harm but strong legal control over a major

provider may be able to obtain decisive evidence quickly, creating a functional advantage that territoriality doctrine does not formally recognize yet practice cannot ignore (Guan, 2025).

A fourth driver is the attribution problem, which interacts with territoriality in a particularly corrosive way. In cyberterrorism, early investigative hypotheses about origin are often probabilistic, inference-heavy, and vulnerable to deception. False flags, spoofed indicators, and the reuse of tooling blur the line between evidence of origin and evidence of imitation. Territorial effects, by contrast, are more readily observable, which tempts states to treat effects as sufficient for jurisdiction even when attribution is weak. That temptation produces a procedural imbalance. A forum may commence a major prosecution based on local disruption, but the evidentiary pathway to a named defendant may require cross-border data, technical expertise, and cooperative disclosure that is not guaranteed (Spáčil, 2024). When cooperation fails, the case risks either collapse or a shift toward lower-quality proof, which raises due process concerns. Territoriality, in other words, can make it easy to assert jurisdiction before it is feasible to litigate responsibly (Fatihah, 2022).

2. The Core Proposal: Functional Control Test (FCT)

The Functional Control Test is designed to answer a practical question that classical jurisdiction doctrine leaves under-specified in cyberterrorism cases: when several states can plausibly point to territory, victims, infrastructure, or security interests, which connection is legally and operationally weighty enough to justify leading the prosecution, and which connections should remain supportive or peripheral. The premise is that cyberterrorism is best understood as a chain of controllable functions rather than a single geographically located act. Jurisdictional legitimacy therefore increases when a state can demonstrate a stronger relationship to the functions that enabled the operation to be initiated, directed, sustained, and evidenced through lawful process. The test does not deny the classical bases of jurisdiction (Wheatley, 2023). It disciplines their application by requiring the state to translate abstract bases such as “effects” or “protection” into concrete, operation-linked control factors that can be articulated, contested, and reviewed (Kadir, 2026a).

Functional control, in this article, refers to the demonstrable ability of an actor or an entity subject to a state’s authority to initiate, steer, maintain, or terminate the material components of a cyberterrorism operation. The concept is intentionally operational rather than metaphysical. It focuses on decision points and leverage points: who could have started the operation, who issued instructions, who controlled the channels that carried those instructions, who possessed privileges over the infrastructure that hosted or propagated the attack, and who could have stopped or materially constrained the operation. Functional control can be direct, as when an operator has administrative access to a command-and-control panel, controls a domain used for payload distribution, or holds cloud identities that allow deployment. It can also be mediated, as when control is exercised through persons or entities that are legally subject to a forum’s regulatory and coercive powers, such as service providers that can preserve logs, disable accounts, or disclose subscriber data under domestic process (Liat & Wahyuningtyas, 2025). In both instances, the legal relevance lies in the capacity to link the forum to the operational mechanics and to the evidence required for adjudication, not merely to downstream harm.

The test is structured as a weighted, reason-giving assessment organized around four elements. The elements are designed to be sufficiently specific to reduce arbitrariness, yet flexible enough to accommodate diverse operational patterns. The elements are not rigidly cumulative in the sense that failure on any single element automatically defeats jurisdiction. Instead, the test generates a structured justification for prioritization: a forum with consistently strong control factors across the elements has a more legitimate claim to be the primary prosecuting jurisdiction; a forum with moderate factors may claim concurrent jurisdiction; a forum with weak or speculative factors should remain peripheral, relying on cooperation and assistance rather than leading.

The first element is Operational Direction. This element captures whether the core decision-making and orchestration of the cyberterrorism operation is meaningfully connected to the forum. The strongest indicators are those tied to command and control: evidence that the operator or leadership executed tasking, updated instructions, scheduled campaigns, assigned targets, or managed operational security from within the forum or through identities and systems that are attributable to persons located there. Where physical location is uncertain, the inquiry looks for functional proxies of direction that are legally and technically meaningful, such as authenticated administrative sessions to a control panel,

deployment keys, cryptographic signing of payload updates, or coordination artefacts that demonstrate authorship and authority. Importantly, the element does not treat mere transit through infrastructure as operational direction. A routing path that passes through a state does not establish direction; direction is established by controllable decision points that shaped the operation.

The second element is Infrastructure Leverage. Cyberterrorism depends on infrastructure, but not every infrastructural touchpoint is equally significant. This element distinguishes between incidental use and leverage-conferring control. High-value indicators include administrative privileges over hosting environments, ownership or control of domains and certificates, control of cloud identity and access management roles, the ability to configure load balancers or content distribution rules for payload delivery, and the capacity to manage botnet enrolment, updates, and kill-switches. The key question is whether the forum is linked to the infrastructure in a way that reflects meaningful power over the operation's continuation. A compromised device located in a state may be part of the operation, but unless the operator's leverage over that device is part of a broader control structure that is itself connected to the forum, the mere presence of the device should carry limited jurisdictional weight. This is where the test deliberately resists the inflationary logic of territoriality-by-compromise (Bederna & Rajnai, 2022).

The third element is Targeting and Foreseeability of Effects. This element incorporates the normative intuition that victims and harms matter, while avoiding the doctrinal trap of treating diffuse effects as automatically dispositive. The inquiry asks whether the operation was targeted at the forum's protected interests in a way that was foreseeable and deliberate, rather than merely incidental. Strong indicators include selection of local critical infrastructure as an objective, tailored reconnaissance against local systems, the use of language, timing, or operational choices aimed at coercing the forum's government or intimidating the forum's public, and the presence of specific demands directed at the forum. This element is also sensitive to the gravity of the effect. A minimal disruption with generalized rhetorical intent should not justify the same jurisdictional priority as a sustained campaign aimed at disabling essential services. The functional point is to translate "effects" into a structured inquiry about intentional targeting and predictable coercive harm, so that the forum's claim is anchored in a legally intelligible relationship between the operation's purpose and the forum's interests.

The fourth element is Evidentiary and Compliance Reach. Cyberterrorism prosecutions often succeed or fail based on whether the prosecuting forum can lawfully secure the decisive artefacts of proof. This element assesses whether the forum has a realistic pathway to obtain and authenticate the evidence necessary to link the operation to specific defendants while respecting sovereignty and due process (Miller, 2023). Indicators include the location of key service providers under the forum's legal authority, the forum's capacity to compel preservation and disclosure of logs and subscriber data, the feasibility of maintaining chain-of-custody standards recognized by the forum's courts, and the availability of robust mutual assistance arrangements that can deliver evidence within operational timelines (Kusak, 2024). This element is not an invitation to privilege "provider domicile" as an automatic jurisdictional trump card. Its role is to prevent a jurisdictional choice that is formally plausible but practically incapable of meeting proof burdens without unlawful shortcuts. A forum that cannot plausibly gather the evidence without conducting unilateral remote searches in another state should not be prioritized as primary, even if it can assert territorial effects (Guo, 2023).

The test yields three jurisdictional categories. Primary jurisdiction is appropriate where a forum scores strongly on Operational Direction and Infrastructure Leverage, and has either strong Targeting/Foreseeability or strong Evidentiary/Compliance Reach. In practice, this will often be the state most closely linked to the operator's command structure or the state that can lawfully compel the core evidence while also showing a non-trivial targeting connection. Concurrent jurisdiction is appropriate where a forum can show deliberate targeting and serious local effects, or strong evidentiary reach, but lacks the strongest direction/leverage links. Peripheral interest describes forums that can point to some impact or incidental infrastructural touchpoints but cannot show meaningful operational control or feasible evidentiary pathways. Peripheral forums should be treated as stakeholders in cooperation rather than as leading prosecutors.

Two features are essential to keeping the test normatively compatible with international law constraints. First, the Functional Control Test is a prioritization method for jurisdiction to prescribe and adjudicate, not a blanket authorization for jurisdiction to enforce extraterritorially. Even where a forum is classified as primary, coercive investigative acts on the territory of another state remain constrained

by sovereignty and non-intervention and ordinarily require consent, cooperation, or a clear legal basis under applicable arrangements. Second, the test imposes a reason-giving discipline. A state asserting primary jurisdiction should be able to articulate, in a way that can be scrutinized judicially and diplomatically, which functional control indicators support its claim and why alternative claimants are weaker. That discipline matters for legitimacy because cyberterrorism cases are prone to security-driven shortcuts. Requiring a structured showing of operational direction, infrastructural leverage, targeting, and evidentiary feasibility makes it harder to justify expansive extraterritorial prosecutions grounded solely in generalized harm or abstract security rhetoric.

3. Application to Cross-Border Operational Scenarios

To show that the Functional Control Test does real work, it must be applied to operational patterns that routinely generate competing jurisdictional claims. The point is not to produce a single mechanically "correct" forum in every case, but to demonstrate that the test yields a disciplined prioritization logic that is harder to manipulate than effects-only territoriality and less politically malleable than unbounded protective claims. The scenarios below are stylized but realistic enough to capture the recurring frictions in cyberterrorism investigations and prosecutions (Muhtada et al., 2023).

Consider first a botnet-enabled attack against a metropolitan transport system. The disruption is visible in State A, where ticketing and signaling systems are degraded and public fear is amplified by a manifesto demanding political concessions. Forensic traces show that the traffic originated from tens of thousands of compromised devices scattered across States B through N. A command-and-control panel appears to be hosted by a "bulletproof" provider in State C, while payment for infrastructure was made through a cryptocurrency exchange subject to regulation in State D. Investigators in State A claim objective territoriality and protective jurisdiction because the target is critical infrastructure and the effect is coercive fear. States B through N could claim territoriality as well because their territory hosted parts of the botnet. State C could claim territoriality due to hosting of command infrastructure. State D could claim a jurisdictional interest based on its regulatory control over payment and subscriber records.

Under a functional control analysis, the botnet nodes in States B through N typically carry low jurisdictional weight because they represent coerced intermediaries rather than operational direction or meaningful leverage. Their presence indicates where the operation propagated, not where it was controlled. The more legally salient connection lies in who directed the botnet and who controlled the infrastructure that enabled direction. If the evidence shows administrative sessions to the command-and-control panel attributable to an operator located in State X, Operational Direction and Infrastructure Leverage point strongly to State X as the primary prosecuting forum, assuming State X can lawfully obtain or compel the key logs and subscriber data needed to identify the operator. If the operator's physical location remains uncertain but State C can lawfully compel the hosting provider to preserve and disclose control-panel logs and account identifiers, State C may have a strong Evidentiary and Compliance Reach that supports at least concurrent jurisdiction and, in some cases, primary jurisdiction if it can also connect the operator to its territory or to identities and assets subject to its authority. State A retains a strong Targeting and Foreseeability connection because the transport system is a deliberate local target and the coercive effect is not incidental; this ordinarily justifies concurrent jurisdiction and a robust claim to participate, but it does not automatically entitle State A to lead if it cannot secure the decisive evidence without external compulsion. The test therefore does two things simultaneously: it prevents "territoriality-by-compromise" from producing dozens of inflated territorial claims, and it forces the victim state to articulate, beyond harm, whether it can credibly assemble proof and custody through lawful cooperation (Rahardjo, 2022).

A second scenario involves cloud-based orchestration and serverless execution aimed at disabling emergency communications across multiple cities. The adversary uses a cloud account to deploy functions that dynamically pull malicious modules from object storage, rotate endpoints, and trigger waves of requests that overwhelm systems. Data and compute are provisioned across multiple regions; the cloud provider's corporate headquarters is in State E, but the region serving the most traffic at the moment of attack is in State F. The operator is physically in State G, using layered anonymization and rented credentials. Several states suffer disruptions and claim objective territoriality based on local effects. State E asserts strong jurisdiction on the basis that it can compel the provider. State F asserts territoriality because its data centers were used. State G is not yet confident it can attribute the operation to a person within its territory.

The Functional Control Test resists treating transient compute location as determinative. The fact that a region in State F served traffic is an infrastructural touchpoint, but it may be incidental to the operator's decisions if the cloud service automatically selected region placement or failover. The more probative locus of functional control is the cloud identity and access management privileges that enabled deployment and rotation. If State E can compel the cloud provider to produce audit trails, authentication logs, billing records, and account recovery events, it may have strong Evidentiary and Compliance Reach that makes it an effective lead forum—provided it can link those records to an identifiable actor and can supply procedural safeguards. If State G can demonstrate that the operator's operational direction occurred from within its territory—such as device artefacts, local network traces, or seized devices tied to account administration—then Operational Direction points to State G as a strong candidate for primary jurisdiction. States suffering disruptions will likely satisfy Targeting and Foreseeability if evidence indicates deliberate selection of their emergency systems rather than generalized disruption, but again the test discourages those states from claiming primacy solely on the basis of harm when the evidentiary center of gravity sits with the cloud provider and the operator's control artifacts (Garcia et al., 2024).

A third scenario concerns coordination through end-to-end encrypted messaging and platform-mediated recruitment that precedes a cyberterrorism attack. Suppose an extremist network uses an encrypted messaging platform to recruit technical volunteers, distribute operational guidelines, and direct a timed cyber campaign against a government portal in State H. The platform is incorporated in State I, but the encryption architecture limits content access; only certain metadata may be obtainable. The operational infrastructure for the attack itself—domains, hosting, and botnet rental—touches States J and K. State H claims protective jurisdiction and objective territoriality because the government portal is targeted and public intimidation is part of the strategy. State I faces pressure to lead or to act because the platform is domiciled there.

Here the Functional Control Test prevents the common mistake of equating platform domicile with operational control over the offence. If the platform cannot access content and retains only limited metadata, State I's Infrastructure Leverage over the operation may be weaker than assumed, even if its compliance reach is meaningful for certain kinds of proof. State I may still have an important assistance role by preserving metadata, disclosing account registration information, and supporting attribution, but it should not automatically be treated as the primary prosecuting forum absent stronger indicators of Operational Direction connected to its territory or persons subject to its authority (Setiawan, 2024). State H likely has a strong Targeting and Foreseeability nexus because it is the intended coercion target, and it may have additional strength if local investigative steps can connect suspects to devices, local network access, or financial trails. States J and K may have meaningful leverage if they can compel hosting and registrar records that reveal who controlled domains, certificates, or command infrastructure (Wijayanto, 2023). The test thus yields a differentiated picture: State H may be a plausible primary forum if it can secure attribution and key evidence through cooperation; otherwise, a state with stronger evidentiary reach over infrastructure control may be better placed to lead, with State H retaining a strong concurrent interest and victim-centered participation .

Across these scenarios, the common pattern is that "where harm is felt" and "where infrastructure sits" do not always identify "where control resides" or "where proof can be lawfully assembled." The Functional Control Test turns that observation into a disciplined prioritization method. It assigns limited weight to coerced intermediaries and incidental routing, increases weight where operational direction and infrastructure leverage are demonstrable, treats targeting as a necessary constraint against purely provider-centric prosecutions, and integrates evidentiary feasibility to deter forums from leading cases they can sustain only through unlawful shortcuts. That is precisely the type of structured reasoning needed to manage concurrency in cyberterrorism without normalizing overreach or accepting impunity as inevitable (Kadir, 2026b).

CONCLUSION

The core claim of this article is that cyberterrorism exposes a structural mismatch between territorial instincts in criminal jurisdiction and the functional reality of digitally mediated operations. Territoriality and effects-based reasoning remain part of the jurisdictional vocabulary, but in distributed attacks they frequently produce either diluted claims grounded in incidental infrastructure or inflated claims grounded in expansive narratives of harm and security. The Functional Control Test offers a

more disciplined nexus assessment by requiring states to justify prosecutorial primacy through demonstrable operational direction, meaningful infrastructure leverage, deliberate targeting and foreseeable coercive effects, and a lawful, feasible pathway to secure decisive evidence. By ranking claims as primary, concurrent, or peripheral, the test manages concurrency rather than denying it, and it reduces incentives for forum opportunism while closing predictable accountability gaps.

At the same time, the test is designed to fit within the constraints that make international criminal law stable: sovereignty, non-intervention, and the separation between prescription/adjudication and enforcement. A strong functional control nexus can justify leading prosecution, but it does not normalize unilateral cross-border coercion or "remote policing" beyond borders. Instead, it shifts the burden toward reason-giving jurisdictional choices that can be scrutinized, and toward cooperation pathways that preserve evidentiary integrity and fair process. In a domain where technical capability often tempts legal shortcuts, a control-oriented jurisdictional method provides a defensible way to pursue effective cyberterrorism accountability without letting necessity rhetoric erode the limits that keep transnational criminal justice legitimate.

REFERENCES

Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, *29*(2), 118–153. https://doi.org/10.1093/ijlit/eaab001

Beckerman, C. E. (2022). Is there a cyber security dilemma? *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac012

Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, *3*(1), 35–49. https://doi.org/10.1365/s43439-022-00048-9

Eichensehr, K. E. (2022). Back to the roots: The laws of neutrality and the future of due diligence in cyberspace. *European Journal of International Law*, *33*(3), 789–819.

Fatihah, C. Y. N. (2022). Indonesia's Approach on Cyberattack Attribution through its Foreign Policy. *Global Legal Review*, *2*(2), 121. https://doi.org/10.19166/glr.v2i2.5140

Garcia, G. S., íno-Solano, A. V., & Salazar, B. P. (2024). The Debate Concerning Deviance and Divergence: A New Theoretic Proposal. *Oñatio Socio-Legal Series*, *14*(2), 505–529.

Guan, C. (2025). Cross-border cybercrime digital evidence: Current research and fundamental categories. *Modern Law Research*, *6*(4).

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Kadir, Z. K. (2026a). Narrative Closure in Honor killing Cases: How Judgments Stabilise Meaning, Eliminate Ambiguity, and Produce Sentencing Certainty. *Punggawa Law Review*, *1*(1), 1–10.

Kadir, Z. K. (2026b). Neurocriminology and the Next Generation of Criminological Theory: Integration, Limits, and Ethical Risks. *Punggawa Global Research: Jurnal Multidisiplin*, *1*(1), 1–8.

Kusak, M. (2024). EU Cross-Border Gathering and Admissibility of Electronic Content Data. *European Journal of Crime, Criminal Law and Criminal Justice*, *32*(2), 126–155. https://doi.org/10.1163/15718174-bja10054

Liat, K. E., & Wahyuningtyas, S. Y. (2025). PELINDUNGAN DATA PRIBADI DALAM BISNIS KOMPUTASI AWAN DI INDONESIA: TRANSFER DATA LINTAS NEGARA DAN AKSES OLEH OTORITAS PUBLIK. *Refleksi Hukum: Jurnal Ilmu Hukum*, *9*(2), 195–214. https://doi.org/10.24246/jrh.2025.v9.i2.p195-214

Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, *6*, 100296. https://doi.org/10.1016/j.fsisyn.2022.100296

Muhtada, D., Al-Fatih, S., & Yuliantoro, N. R. (2023). The direction of Indonesia's legal policy on the ASEAN Mutual Legal Assistance Treaty in criminal matters: A path to law reform in cross-border crime enforcement in Southeast Asia. *The Direction of Indonesia's Legal Policy on the ASEAN Mutual Legal Assistance Treaty in Criminal Matters: A Path to Law Reform in Cross-Border Crime Enforcement in Southeast Asia*, *5*(2), 749–780.

Nurkhasanah, K. I., & Prasetyo, Z. M. (2024). Law Enforcement of State Jurisdiction in Hacking Crimes. *Indonesian Journal of Applied and Industrial Sciences (ESA)*, *3*(3), 319–328. https://doi.org/10.55927/esa.v3i3.9438

Olber, P. (2021). The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities. *Journal of Digital Forensics, Security and Law*, *16*(2). https://doi.org/10.58940/1558-7223.1700

Osula, A.-M., Kasper, A., & Kajander, A. (2022). EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, *16*(1), 89–121.

Rahardjo, A. (2022). Legal complexity in dealing with cyber crime in Indonesia. *Research Horizon*, *2*(6), 597–606.

Rusdianto, R., & Risnain, Muh. (2023). Penerapan Prinsip Extraterritorial Jurisdiction Dalam Memerangi Tindak Pidana Siber. *Mataram Journal of International Law*, *1*(1). https://doi.org/10.29303/majil.v1i1.2532

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, *24*(1), 537–550.

Schmitt, B. (2021). Legal Diversity at the International Criminal Court. *Journal of International Criminal Justice*, *19*(3), 485–510. https://doi.org/10.1093/jicj/mqab038

Setiawan, A. (2024). End-to-end encryption: Apakah ini sebuah ancaman? *Jurnal Analis Kebijakan*, *8*(2), 233–240.

Spáčil, J. (2024). Attribution of Cyber Operations: Technical, Legal and Political Perspectives. *International and Comparative Law Review*, *24*(2), 150–168. https://doi.org/10.2478/iclr-2024-0022

Wheatley, S. (2023). Election hacking, the rule of sovereignty, and deductive reasoning in customary international law. *Leiden Journal of International Law*, *36*(3), 675–698. https://doi.org/10.1017/S0922156523000092

Wijayanto. (2023). Safe harbor principle, exclusion of criminal liability for platform service providers. *Indonesian Journal of Criminal Law Studies*, *8*(2), 187–208.