A Hybrid Cyber Defense Framework for Indonesia's Military Integration into National Cyber Resilience: A Counterfactual Stress-Test

Fibriansyah Fatahillah and Timothy Shives
Naval Post-graduate School, Monterey, California, USA

fibriansyah.fatahillah.id@nps.edu
timothy.shives@nps.edu

Abstract: The June 2024 ransomware attack on Indonesia's National Data Center (*PDN*) disrupted hundreds of public services and exposed that the country's cyber vulnerability extended beyond weak technical controls to include fragmented authority, unclear mandates, and slow coordination among state actors, which plausibly amplified the scale and duration of disruption. Existing work on Indonesia's cyber defense and national cyber resilience often treats technological upgrades and institutional reform separately and rarely tests how alternative governance architectures might have altered the trajectory of a real incident. This paper asks whether a hybrid civil-military cyber defense framework could have reduced the operational impact of the *PDN* incident by mitigating coordination failures across detection, containment, and recovery phases. Drawing on open-source reporting, the study reconstructs an incident timeline and identifies three failure nodes: detection delay, containment delay, and recovery failure linked to backup governance. Conceptually, it refines existing socio-technical accounts by formalizing coordination failure as a second-order amplifier of cyber incident severity that links fragmented authority to decision latency and expanded incident impact once attackers gain a foothold. Building on prior work that designed a cyber defense framework for the Indonesian Armed Forces, the paper extends this architecture to a national civil-military setting by specifying a Hybrid Cyber Defense Framework centered on a civilian-led National Cyber Security Coordination Center (NCCC) with unified incident command and a Joint Cyber Defense Task Force (JCDTF) providing surge technical capacity under democratic safeguards. Using Counterfactual Process Tracing (CPT), grounded in an interventionist theory of causation, the analysis stress-tests this framework against the PDN timeline, holding baseline technical weaknesses constant while minimally rewiring decision paths and information flows at the three failure nodes. Analog evidence from NATO and Singapore suggests integrated monitoring, pre-designated leadership, and joint exercises can compress response cycles without replacing technical controls. The paper offers a mechanism-based template for stress-testing national cyber governance arrangements against concrete incident trajectories and clarifies the democratic boundary conditions under which hybrid civil-military integration is more likely to strengthen cyber resilience.

Keywords: Cyber defense, National resilience, JCDTF, NCCC, Indonesia, Counterfactual process tracing, *RUU KKS*

1. Introduction

In June 2024, a ransomware attack on the National Data Center (*Pusat Data Nasional/PDN*) disrupted hundreds of public services and exposed deep structural weaknesses in Indonesia's cyber governance (Antoniuk, 2024). While technical deficiencies, such as inadequate patching, disabled security features, and absent backups were immediate causes, they do not fully explain the scale and duration of the crisis. The incident revealed a deeper systemic issue: fragmented authority and poor coordination among key institutions, including the Ministry of Communication and Informatics (*Kominfo*), the National Cyber and Crypto Agency (*Badan Sandi dan Siber Nasional/BSSN*), and state-owned infrastructure providers (Nugroho, 2024).

This paper asks whether a hybrid civil-military cyber defense framework could have reduced the operational impact of the 2024 *PDN* ransomware incident by mitigating coordination failures among Indonesian state actors. First, we refine socio-technical accounts by formalising coordination failure as a second-order amplifier linking fragmented authority to decision latency and incident impact. Second, we extend our earlier, TNI-focused cyber defence framework to the national level by specifying a hybrid civil-military architecture in which a civilian-led National Cyber Security Coordination Center (NCCC) exercises unified incident command while a Joint Cyber Defense Task Force (JCDTF) provides surge technical capacity under democratic safeguards (Shives & Fatahillah, 2026). Third, we use Counterfactual Process Tracing (CPT) to mechanism-test this hybrid architecture against three empirically identified failure nodes—detection delay, containment delay, and recovery failure— showing how minimally rewired decision paths could constrain escalation without assuming away underlying technical weaknesses.

2. Literature Review and Conceptual Background

While cybersecurity research has often focused on technical controls, large-scale incidents increasingly show that organizational structures and decision processes strongly shape the severity and duration of disruption. (Khair et al., 2025). Priyandita and Lebang (2025) argue that overlapping mandates and unclear hierarchies

between *Kominfo*, *BSSN*, law-enforcement bodies, and military cyber units produce coordination gaps and decision latency during crises. Debates on Indonesia's Cybersecurity and Resilience Bill (RUU KKS) highlight concerns that efforts to centralize authority and integrate military capabilities into civilian cyber governance (Riani Sanusi Putri, 2026; Wahyudi Djafar & Al Araf, 2025)

This literature suggests that civil-military integration in cyberspace is not inherently beneficial or harmful; its effects depend on how command structures, oversight mechanisms, and legal mandates are designed and implemented (CSA Singapore, 2026). The present study adopts this conditional view and explicitly treats democratic governance as a boundary condition for any proposed hybrid framework: the same architecture that reduces coordination failures can also concentrate power and reduce transparency if not paired with robust checks and balances (Lebang, 2025).

This study builds on Shives and Fatahillah's (2026) Indonesian Armed Forces (*Tentara Nasional Indonesia*) *TNI*-focused cyber defence framework by shifting from military-internal design to hybrid civil-military governance at the national level and by stress-testing selected design features against the concrete failure modes observed in the *PDN* ransomware incident. Rather than proposing an ideal end-state architecture in the abstract, it uses Counterfactual Process Tracing to assess how NCCC and JCDTF would interact with existing institutions under Indonesia's evolving Cybersecurity and Resilience Bill (*RUU KKS*).

3. Theoretical Framework: Coordination as an Incident Amplifier

3.1 Coordination Failure as a Second-Order Amplifier

Building on Indonesian and comparative studies that highlight fragmentation and overlapping mandates as core governance challenges, this paper conceptualizes coordination failure as a second-order amplifier of cyber incident impact (Lebang, 2025; Nugroho, 2024). In this view, foundational technical weaknesses such as absent backups, disabled security controls, or unpatched systems remain first-order drivers of vulnerability, but coordination plausibly conditions how far and how long an incident escalates once initial compromise has occurred, rather than determining the likelihood of compromise itself (Antoniuk, 2024; Sangfor Technologies, 2024). The central causal chain is:

Fragmented Authority → Decision Latency → Expanded Incident Impact

Fragmented authority arises when multiple organizations share responsibility without a clear hierarchy or unified operational structure (Priyandita & Lebang, 2025). Decision latency captures the additional time required to negotiate responsibilities, obtain authorization for containment actions, and mobilize resources across institutional boundaries (Runhardt, 2024). Expanded incident impact refers to wider service disruption, longer outage duration, and more extensive data or system compromise than would have occurred under faster, more coherent decision-making (Khair et al., 2025)

From this chain, we derive two guiding propositions for the PDN case:

1. P1 (Authority and latency): Where incident-response authority is fragmented across agencies, the time between initial detection and issuance of system-wide containment orders increases.
2. P2 (Latency and impact): Longer decision latency is positively associated with the scope and duration of disruption in critical services once initial compromise has occurred.

These propositions are not intended to be statistically general but to structure a within-case evaluation of how authority arrangements influenced the trajectory of the PDN ransomware incident.

3.2 The Hybrid Cyber Defense Framework as an Intervention

The Hybrid Cyber Defense Framework proposed in this paper is designed to intervene directly in the coordination mechanism rather than in the technical vulnerability space. It consists of two core institutional components: NCCC with authority to direct national cyber incident response, and JCDTF that integrates military cyber units with civilian experts to provide surge technical capacity.

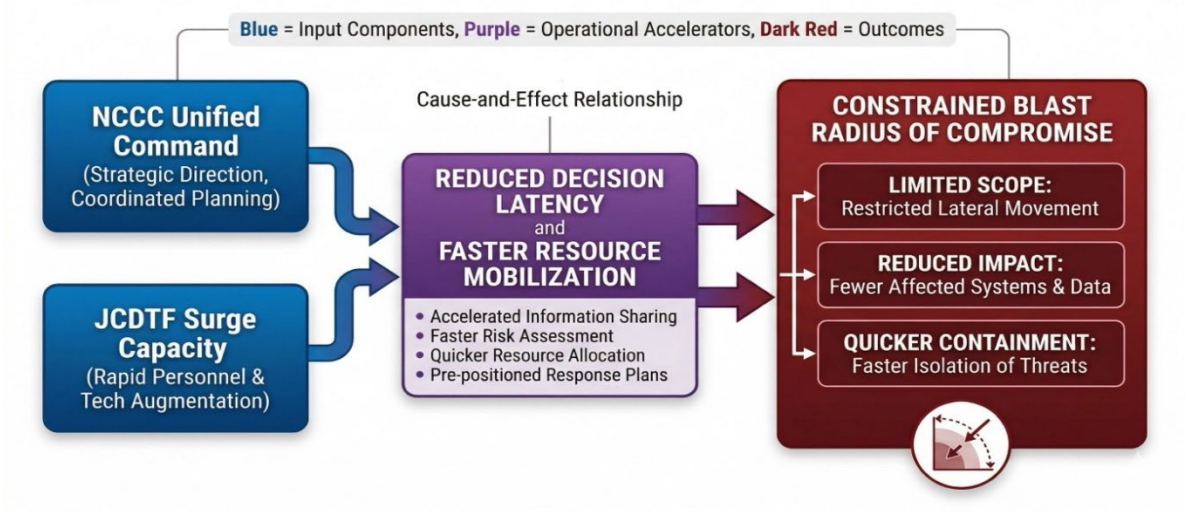

Figure 1: Operational Mechanism of the Hybrid Cyber Defense Framework

As illustrated in Figure 1, the integration of NCCC Unified Command with JCDTF surge capabilities creates a synergistic effect that directly reduces decision latency, thereby constraining the blast radius of a cyber compromise. The framework is explicitly conditional: it cannot compensate for missing backups or unpatched systems, but it can alter how quickly such deficiencies are detected and how effectively their consequences are managed (Antoniuk, 2024; Sangfor Technologies, 2024). Coordination, in other words, does not prevent initial compromise, but it can plausibly limit the temporal and organizational scope of damage (Khair et al., 2025).

4. Methodology: Counterfactual Process Tracing (CPT)

4.1 Rationale for CPT

This study employs Counterfactual Process Tracing (CPT), grounded in an interventionist theory of causation, to evaluate how alternative governance architectures might have altered the dynamics of the *PDN* ransomware incident (Runhardt, 2024). Rather than estimating correlations, CPT examines within-case mechanisms and whether interventions could change outcomes without violating established facts. In our case, the intervention is the introduction of a hybrid NCCC-JCDTF framework that modifies authority structures and coordination mechanisms but leaves baseline technical vulnerabilities unchanged.

4.2 Data and Source Base

The empirical baseline is constructed from official statements, technical advisories, and investigative reporting on *PDN* operations and incident response. We compile these sources into a timeline recording technical events (such as initial disruption, ransom demand, and restoration milestones), institutional responses, and public communications. Where sources diverge, we retain ranges rather than a single estimate. The source base is incomplete and biased: official accounts may understate coordination problems, while others may emphasize technical or political failures. We interpret the timeline as a conservative representation of coordination failure and cross-validate key claims across sources.

4.3 Analytical procedure

The CPT analysis proceeds in four steps:

- First, we synthesize the collected material into a chronological incident timeline (Table 1) and identify key decision points and delays between technical events and institutional responses.
- Second, we identify failure nodes where coordination and authority appear to have materially shaped outcomes and derive three critical nodes: detection delay, containment delay, and recovery failure due to unverified backup governance.
- Third, drawing on the proposed Hybrid Cyber Defense Framework, we specify a counterfactual architecture where NCCC exercises unified command and JCDTF provides surge capacity (Shives & Fatahillah, 2026). For each failure node, we model how this architecture would rewire decision paths and information flows via three mechanisms: decision latency, resource-mobilization speed, and information integration, while holding baseline technical conditions constant.

- Fourth, we conduct counterfactual evaluation and assess competing explanations. For each node, we compare the observed sequence with the minimally rewired counterfactual sequence that is consistent with the hybrid architecture and with known technical constraints of the *PDN* environment. We evaluate whether the hybrid model or alternatives, technical failure alone, civilian-only governance reform, or outsourcing to private providers, offers greater mechanism coverage of the observed delays and failures (Lebang, 2025; Priyandita & Lebang, 2025)

A counterfactual claim is accepted only when it (a) does not contradict established facts about PDN infrastructure and the attack, and (b) is supported either by within-case trace evidence or by analog evidence from other national or alliance-level cyber defense arrangements that have implemented comparable coordination mechanisms (Neilsen & Pontbriand, 2025). This counterfactual assumes baseline compliance with NCCC authority; partial compliance or inter-agency resistance would attenuate, but not eliminate, expected reductions in decision latency. At the extreme, where compliance is systematically resisted, no meaningful reduction in coordination latency should be expected. Operationally, we measure decision latency as the elapsed time between first observable anomaly and (i) formal incident recognition and (ii) issuance of cross-agency containment orders, based on open-source timelines. Expanded incident impact is captured through the number and criticality of affected services and the duration of service degradation, while coordination failure is indicated by overlapping mandates, the absence of a single empowered incident commander, and documented episodes of ad hoc or improvised escalation.

5. Empirical Case: The 2024 PDN Ransomware Attack

5.1 Baseline Incident Timeline

The empirical baseline for this study is the June 2024 ransomware attack on Indonesia's National Data Center, which disrupted hundreds of central and local government services across sectors including immigration, licensing, and taxation (Nugroho, 2024). Open-source reporting indicates that attackers maintained undetected access for several days prior to the visible disruption of services, with estimates of persistence ranging from approximately four to seven days (Antoniuk, 2024; Sangfor Technologies, 2024). On the morning of 20 June 2024, service degradation in immigration systems provided the first reported indicator of disruption, yet open-source reporting indicates no evidence of a pre-designated national incident command authority being activated at this stage, suggesting delayed cross-agency coordination.

We treat the persistence window as approximately four to seven days, the escalation lag from first visible disruption to a coherent inter-agency posture as roughly four to six hours, and the interval to public recognition of a ransomware incident as about twenty-four hours, all derived from overlapping but imperfect open-source accounts.

Table 1: *PDN* Ransomware Incident Timeline

Time / Date	Event	Observed Issue
~June 13-17, 2024 (T-7 to T-4 days)	Initial compromise and attacker persistence	Lack of detection; fragmented monitoring (Antoniuk, 2024; Georgia Butler, 2024)
June 20, ~08:00	System disruption detected (immigration services impacted)	No immediate unified response (Nugroho, 2024)
June 20, (T+4-6 hrs)	Initial internal escalation across agencies	Coordination delay; unclear authority (Georgia Butler, 2024)
June 21 (~T+24 hrs)	Public acknowledgment of ransomware attack	Delayed situational awareness (Antoniuk, 2024)
June 24 (T+4 days)	Government refuses ransom demand (~$8M)	Absence of predefined crisis protocol (Nugroho, 2024)
June 25+ (T+1-3 weeks)	Gradual service restoration	Backup failure; slow recovery (Antoniuk, 2024)

5.2 Technical and Governance Characteristics of the Attack

Technically, the *PDN* incident involved a ransomware strain assessed to be derived from, or closely related to, the LockBit 3.0 family, reflecting the increasing accessibility of sophisticated tools through ransomware-as-a-service ecosystems (Sangfor Technologies, 2024). Post-incident analyses indicate that baseline security practices at *PDN* were weak: security features such as Windows Defender were reportedly

disabled on critical systems, network segmentation was limited, and backup regimes were incomplete, unverified, or both (Indosec Summit, 2025). However, the technical characteristics explain the initial compromise but do not, on their own, fully account for the observed delays in detection, containment, and recovery across institutions. The response unfolded in an institutional environment characterized by fragmented cyber governance: responsibility for *PDN* infrastructure, cybersecurity oversight, and incident response was distributed among *Kominfo*, *BSSN*, state-owned telecommunications providers, and sectoral agencies whose services depended on *PDN* (Nugroho, 2024; Priyandita & Lebang, 2025). Reports suggest that no single body had the undisputed authority to declare a national-level cyber emergency, direct cross-agency containment actions, or centrally coordinate communication with affected stakeholders. Commentators describe the government's crisis posture during the first days as fragmented and improvisational, highlighting instances where ministries issued overlapping or partially contradictory public statements and where ad hoc coordination groups were created only after disruption had spread (Lebang, 2025). These observable traces reinforce the interpretation of coordination failure as an active mechanism rather than a purely retrospective label.

5.3 Identification of Critical Failure Nodes

Within this baseline, three empirical failure nodes are particularly salient for a mechanism-based analysis. First, detection delay: attacker persistence for several days prior to activation indicates significant blind spots in monitoring and anomaly detection, especially across organizational boundaries within *PDN*'s infrastructure stack (Antoniuk, 2024; Sangfor Technologies, 2024). Second, containment delay: the multi-hour gap between visible disruption and the establishment of a coherent, inter-agency response structure suggests that authority ambiguity and coordination overhead slowed decisions to isolate affected systems and mobilize specialized technical teams (Nugroho, 2024; Priyandita & Lebang, 2025). Third, recovery failure: the prolonged and uneven restoration of services reflects not only missing or corrupted backups but also the absence of a tested, cross-government recovery governance model for prioritizing services, validating restored data, and communicating residual risk to the public (Indosec Summit, 2025; Sangfor Technologies, 2024).

These three nodes: detection delay, containment delay, and recovery failures represent points in the incident trajectory where coordination mechanisms and authority structures plausibly shaped outcomes above and beyond the underlying technical vulnerabilities, and where a hybrid civil-military governance framework could, in principle, have altered decision latency, resource mobilization, and information integration (Nugroho, 2024; Shives & Fatahillah, 2026). The counterfactual assumes baseline compliance with NCCC authority; partial compliance or inter-agency resistance would attenuate, but not eliminate, expected reductions in decision latency.

6. Counterfactual Analysis: Stress-Testing the Hybrid Framework

In applying Counterfactual Process Tracing, each hypothesized mechanism at the three failure nodes is evaluated using hoop-type and smoking-gun-type tests, drawing on both *PDN* evidence and analog national-level cyber operations in NATO and Singapore. The explanatory value of the hybrid framework would be weakened if comparable incidents under unified command structures exhibited similar multi-day detection fragmentation or multi-hour authorization delays

6.1 Detection Phase: Integrated Monitoring and Decision Latency

In the observed *PDN* case, detection capabilities were distributed across multiple agencies and operators without effective integration of logs, alerts, or anomaly reports. This fragmentation plausibly contributed to visibility gaps across organizational boundaries, within which attackers maintained persistence for several days prior to ransomware activation, despite observable disruptions in individual subsystems. Under the proposed Hybrid Cyber Defense Framework, NCCC would serve as a central fusion point for monitoring data from critical government infrastructures, including *PDN* (Shives & Fatahillah, 2026; Singapore MINDEF, 2026). Sectoral teams and JCDTF would provide additional analytic capacity (CSA Singapore, 2026). Evidence from comparable national and alliance-level arrangements, such as NATO's integrated cyber defense of civilian critical infrastructure and Singapore's sectoral cyber defense teams, suggests such fusion mechanisms reduce time to formal incident recognition by minimizing organizational boundaries an alert must traverse (Neilsen & Pontbriand, 2025). For example, in CSA Singapore's operation against APT actor UNC3886, integrated sectoral teams and a central fusion center reportedly compressed cross-sector detection and response cycles from multi-day coordination to within roughly 24 hours in a higher-capacity setting, illustrating mechanism feasibility rather than directly transferable performance expectations. However, the magnitude of these effects is conditional on baseline

institutional and technical capacity, and analog comparisons to higher-capacity systems such as Singapore or NATO should be interpreted as directional rather than directly transferable.

The NCCC does not generate detection signals but reduces time to aggregate and escalate distributed anomaly indicators into a recognized incident. While precise counterfactual timing cannot be established, analog evidence suggests that integrated coordination mechanisms can plausibly compress inter-agency escalation cycles from multi-hour delays to a low-hour range, and reduce cross-sector detection recognition from multi-day fragmentation to within approximately 24 hours under comparable conditions (Neilsen & Pontbriand, 2025).

6.2 Containment Phase: Unified Command and Authorization Delay

Containment in the *PDN* incident was hindered by unclear authority and the need to negotiate responsibilities among multiple ministries, agencies, and operators before decisive action. Reports describe several hours between the first visible service disruptions and the emergence of a coordinated inter-agency response posture, during which affected systems remained partially exposed and lateral movement could continue (Antoniuk, 2024; Nugroho, 2024). In mechanism terms, this reflects a long chain from situational awareness to authorization to act, with no pre-designated incident commander possessing undisputed authority to order isolation, shutdown, or traffic-filtering measures at scale (Priyandita & Lebang, 2025).

The hybrid framework is evaluated here not as an optimal solution, but as a coordination-focused intervention whose explanatory value lies in its ability to account for observed failure nodes relative to competing models (Shives & Fatahillah, 2026). In such an arrangement, containment decisions would flow through a pre-agreed chain of command rather than through ad hoc negotiation among peer agencies, thereby reducing authorization latency where institutional compliance with centralized authority is present (Australian Department of Defence, 2025). Empirical experience from multi-agency cyber operations in other jurisdictions indicates that clearly designated lead authorities and pre-planned rules of engagement can materially shorten decision cycles in the face of fast-moving threats (CSA Singapore, 2026; Neilsen & Pontbriand, 2025). Concretely, under a hybrid model, early immigration-system disruptions could have triggered a predefined national-level incident code mandating immediate isolation of affected *PDN* clusters and tasking of JCDTF teams, rather than relying on improvised escalation chains among peer agencies.

6.3 Recovery Phase: Preparedness, Backup Governance, and Joint Exercises

The *PDN* recovery phase was characterized by incomplete, unverified, or inaccessible backups and by the absence of a clearly defined, cross-government governance model for prioritizing restoration (Indosec Summit, 2025; Sangfor Technologies, 2024). Restoration proceeded unevenly across agencies over one to three weeks, with some services returning relatively quickly and others remaining degraded due to uncertainty about the trustworthiness or completeness of restored datasets (Nugroho, 2024). While these outcomes are rooted in first-order technical weaknesses in backup design and testing, they were compounded by the lack of institutionalized recovery protocols and regular joint exercises at the national level (Fakhreja et al., 2025).

The hybrid framework cannot retroactively create backups that do not exist, but it can shape the governance of preparedness by embedding regular, multi-agency cyber incident exercises and standardized backup verification procedures into the mandates of the NCCC and JCDTF (Shives & Fatahillah, 2026). In the *PDN* counterfactual, a mature hybrid framework would likely have produced two observable differences: first, a higher probability that backups for priority services had been verified through prior exercises; and second, a more coherent and transparent governance structure for orchestrating the restoration process and communicating timelines to stakeholders (Indosec Summit, 2025; Sangfor Technologies, 2024). Even if backups failed, structured recovery governance could reduce uncertainty, shorten outages for critical services, and mitigate secondary political and societal costs (Fakhreja et al., 2025; Nugroho, 2024).

6.4 Relative Plausibility and Competing Explanations

At the same time, the analysis explicitly considers three competing explanations: a technical failure model that attributes the crisis entirely to poor cybersecurity practices and absent backups; a governance-only civilian reform model focused on strengthening *BSSN* and *Kominfo* without military integration; and an outsourcing model that relies primarily on private-sector cybersecurity providers for incident response (Lebang, 2025).

Table 2: Competing Explanations and *PDN* Failure Nodes

Explanation model	Detection delay	Containment delay	Recovery failure
Technical failure	Explains compromise, not multi-day blind spot (Sangfor Technologies, 2024).	Partly explains difficulty, not hours-long lag (Nugroho, 2024).	Strongly explains missing/corrupted backups (Sangfor Technologies, 2024).
Civilian-only governance reform	Reduces some ambiguity, leaves surge capacity vague (Priyandita & Lebang, 2025)	Partially alleviates coordination issues (Lebang, 2025).	Limited leverage beyond core civilian sectors (Indosec Summit, 2025).
Outsourcing to private providers	Improves tooling, adds public-private boundary (Indosec Summit, 2025).	Does little to reduce authorization latency (Riani Sanusi Putri, 2026)	Recovery still depends on state priorities (Lebang, 2025).
Hybrid NCCC/JCDTF framework	Directly targets monitoring integration. (Shives & Fatahillah, 2026)	Provides single commander and surge deployment. (Shives & Fatahillah, 2026)	Embeds joint exercises and backup checks. (Australian Department of Defence, 2025; Singapore MINDEF, 2026)

The technical failure model convincingly explains why the attackers were able to cause severe disruption once inside *PDN*, but it does not account for the multi-day detection gap or the multi-hour coordination lag between visible disruption and a unified response (Antoniuk, 2024). The governance-only civilian reform model could, in principle, reduce some coordination problems, but given existing institutional rivalries and capacity constraints, it may reduce authority ambiguity but offers more limited mechanism coverage for surge technical capacity and rapid cross-sector deployment during crisis conditions (Fakhreja et al., 2025; Priyandita & Lebang, 2025). The outsourcing model may strengthen technical depth but risks reproducing many of the same coordination challenges at the public-private boundary, especially in a crisis involving national-security-sensitive data (Indosec Summit, 2025). Table 2 summarises how each explanation performs against the three empirically identified failure nodes. However, the hybrid model's advantage depends on effective inter-agency integration; in environments where institutional rivalry persists, it may reproduce rather than resolve coordination failures. The hybrid model's effectiveness is therefore contingent rather than universal: where institutional rivalry, legal ambiguity, or low inter-agency trust exceed the coordinating authority of the NCCC, the framework may fail to reduce latency and instead reproduce fragmentation under a more centralized structure.

7. Institutional Feasibility and Democratic Boundary Conditions

The feasibility of implementing the proposed Hybrid Cyber Defense Framework in Indonesia depends on both organizational capacity and democratic safeguards. On the capacity side, existing analyses highlight shortages of specialized cyber personnel within *TNI* and civilian agencies, limited expertise in advanced forensics and threat hunting (Fakhreja et al., 2025; Nugroho, 2024). These constraints reduce the number of staff who can be seconded to an NCCC or JCDTF without degrading existing missions.

The hybrid model partially addresses these gaps by proposing mixed teams that combine military, civilian, and contracted experts and by envisaging a gradual build-out of integrated incident-response platforms under NCCC leadership (Shives & Fatahillah, 2026). However, realizing these benefits requires sustained investment, reform of recruitment and training pipelines, and political willingness to prioritize cyber capacity-building relative to other defense and development demands. The framework should therefore be viewed as a medium-term target rather than a short-term plug-and-play solution.

On the governance side, debates around Indonesia's Cybersecurity and Resilience Bill (*RUU KKS*) underscore the risk that centralizing cyber authority and embedding military capabilities into civilian networks could facilitate surveillance, institutional rivalry, and gradual militarization of the digital domain if as reduced oversight may trade off against faster decision-making, creating tension between operational speed and democratic accountability (Lebang, 2025; Riani Sanusi Putri, 2026). To be both legitimate and operationally effective, the hybrid architecture requires explicit civilian leadership, as weak oversight may reduce inter-agency trust and compliance, thereby reintroducing coordination delays the framework is designed to mitigate. Under these conditions, the hybrid framework remains conditionally feasible: it can plausibly improve detection, containment, and recovery performance in incidents like *PDN*, but only if capacity gaps are addressed and democratic checks evolve in parallel.

8. Discussion and Conclusion

In the PDN case, technical failures function as primary drivers enabling initial compromise, while coordination operates as a second-order amplifier that conditions the duration and spread of disruption rather than its occurrence. By formalizing this relationship as a mechanism linking fragmented authority to decision latency and expanded incident impact, the paper contributes to socio-technical approaches that seek to specify how governance structures shape incident dynamics. The counterfactual stress-test of the Hybrid Cyber Defense Framework shows that a unified NCCC command and JCDTF surge capability suggests that a unified NCCC command and JCDTF surge capability could plausibly reduce decision latency and constrain the organizational and temporal spread of disruption, without altering the initial access vector. The findings emphasize that governance reform cannot substitute for basic technical controls: even in an ideal hybrid architecture, absent backups and unpatched systems would still enable attackers to achieve substantial effects. This effect is conditional and diminishes where coordination mechanisms lack sufficient authority or compliance to override fragmentation. In this case, technical weaknesses function as primary enabling conditions, while coordination operates as a second-order amplifier that explains variation in response speed and disruption duration not accounted for by technical factors alone.

Although the empirical focus is Indonesia's PDN incident, the approach is intended as a reusable template rather than a case-bound story. The core steps: reconstructing a conservative baseline timeline from heterogeneous sources, identifying governance-sensitive failure nodes, specifying a feasible alternative authority architecture, and then subjecting that architecture to CPT-style mechanism tests and comparison with competing explanations can be applied to other national-level incidents in sectors such as healthcare, taxation, or digital identity. For policymakers, this implies three priorities: adopting a civilian-led NCCC with clear authority to declare cyber emergencies, organizing surge capacity in mixed JCDTF teams deployable under transparent rules and logging, and institutionalizing joint exercises, backup verification, and incident-timeline reviews that explicitly target decision latency as a second-order amplifier of impact rather than treating coordination failures as an after-the-fact label. Future work will apply CPT to additional Indonesian incidents and quantify decision latency.

Acknowledgments

The authors express sincere gratitude to the Naval Postgraduate School for academic guidance and resources, and to LPDP for sponsorship.

Ethics Declaration: This research was conducted using publicly available data, including government reports, academic papers, and news articles. As such, it did not involve human subjects or confidential data, and formal ethical clearance was not required.

AI Declaration: Open-source artificial intelligence tools were used solely for proofreading. All analysis, arguments, and conclusions presented in this paper are the original work of the authors or are derived from appropriately cited sources.

References

Antoniuk, D. (2024, June 24). Indonesia's national data center encrypted with LockBit ransomware variant. *The Record*. https://therecord.media/indonesia-national-data-centre-hacked

Australian Department of Defence. (2025, May 30). *Defence Security Principles Framework | Defence*. https://www.defence.gov.au/business-industry/industry-governance/defence-security-principles-framework

CSA Singapore. (2026, February 9). *Largest Multi-Agency Cyber Operation Mounted to Counter Threat Posed by Advanced Persistent Threat (APT) Actor UNC3886 to Singapore's Telecommunications Sector*. Cyber Security Agency of Singapore. https://www.csa.gov.sg/news-events/press-releases/largest-multi-agency-cyber-operation-mounted-to-counter-threat-posed-by-advanced-persistent-threat--apt--actor-unc3886-to-singapore-s-telecommunications-sector/

Fakhreja, R., Umam, K., Zahra, K., & Nurjiah, I. S. (2025). National Cyber Defense: Analysis of Incident Severity Factors Using a Decision Tree. *Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity*, *11*(1), 1–15. https://doi.org/10.33172/jp.v11i1.19798

Georgia Butler. (2024, June 25). *Ransomware incident shuts down Indonesian gov't data center*. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/ransomware-incident-shuts-down-indonesian-govt-data-center/

Indosec Summit. (2025, March 24). The Escalating Cyber Threat in Indonesia: A Wake-Up Call for Digital Security. *IndoSec*. http://indosecsummit.com/the-escalating-cyber-threat-in-indonesia-a-wake-up-call-for-digital-security/

Khair, R., Lubis, H. A. S., & Vickri Febrian. (2025). Blockchain Implementation in the Development of a Zero Trust-Based Cybersecurity Framework at the Indonesian National Data Center. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *7*(1), 105–111. https://doi.org/10.30865/json.v7i1.8932

Lebang, C. G. (2025, March 18). *Indonesia's Cyber Security and Resilience Bill: Strengthening Governance or Expanding Institutional Rivalries?* Https://Www.Lab45.Id/. https://www.lab45.id/detail/298/indonesia-rsquo-s-cyber-security-and-resilience-bill-strengthening-governance-or-expanding-institutional-rivalries

Neilsen, R., & Pontbriand, K. (2025). "Hands off the keyboard": NATO's cyber-defense of civilian critical infrastructure. *Defence Studies*, *25*(3), 519–542. https://doi.org/10.1080/14702436.2025.2454353

Nugroho, Y. (2024, August 8). *Indonesia's National Data Centre Ransomware Attack: A Digital Governance Failure?* FULCRUM. https://fulcrum.sg/indonesias-national-data-centre-ransomware-attack-a-digital-governance-failure/

Priyandita, G., & Lebang, C. G. (2025, April 10). Indonesia's cyber soldiers: Armed without a compass. *The Strategist*. https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/

Riani Sanusi Putri. (2026, February 18). *Why Lokataru Finds Indonesia's Cybersecurity Bill Concerning—News En.tempo.co*. Tempo. https://en.tempo.co/read/2087753/why-lokataru-finds-indonesias-cybersecurity-bill-concerning

Runhardt, R. W. (2024). Concrete Counterfactual Tests for Process Tracing: Defending an Interventionist Potential Outcomes Framework. *Sociological Methods & Research*, *53*(4), 1591–1628. https://doi.org/10.1177/00491241221134523

Sangfor Technologies. (2024). *What is Brain Cipher? The Ransomware that Took Down the Indonesian National Data Center*. https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/what-is-brain-cipher-ransomware-took-down-indonesian-national-data-center

Shives, T., & Fatahillah, F. (2026). A Comprehensive Cyber Defense Framework for the Indonesian National Armed Forces: Bridging Governance Gaps for National and ASEAN Cyber Resilience. *The Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026)*, 751–758.

Singapore MINDEF. (2026, February 27). *Fact Sheet: Cyber Defence Test and Experimentation Centre (CyTEC) and Sectoral Cyber Defence Teams (SCDTs)*. Ministry of Defence. https://www.mindef.gov.sg/news-and-events/latest-releases/27feb26-fs2/

Wahyudi Djafar & Al Araf. (2025, October 28). *The militarization of Indonesia's cybersecurity framework—Academia—The Jakarta Post*. The Jakarta Post. https://www.thejakartapost.com/opinion/2025/10/28/the-militarization-of-indonesias-cybersecurity-framework.html