

Public Administration's Function in Addressing Cybercrime: Evaluating Indonesia's Regulatory and Legal Structures

Bayu Erlangga¹

¹ Universitas Negeri Malang, Malang, Indonesia

Abstract

Article history:

Received: January 5, 2024
Revised: February 2, 2024
Accepted: April 22, 2024
Published: June 30, 2024

Keywords:

Digital Offenses, Public Governance,
Regulatory Framework,
Cybersecurity Policy, Indonesian
Law.

Identifier:

Zera Open
Page: 30-57
<https://zeraopen.com/journal/jclis>

The proliferation of internet connectivity and rapid technological advancements have inadvertently facilitated the circumvention of legal statutes by cyber offenders, escalating cyber-related infractions throughout Indonesia. While various policies and legislative instruments have been established to mitigate these digital threats, their operational efficacy remains suboptimal. This inquiry scrutinizes the integral function of public governance and administrative bodies in counteracting cybercrime within Indonesia through a critical examination of the extant regulatory architecture. Employing a normative juridical methodology underpinned by a qualitative paradigm, this investigation derives its analysis from primary legal repositories, including statutory enactments, governmental decrees, and judicial precedents, and secondary scholarly discourse. The analysis elucidates that Indonesia possesses a relatively exhaustive compendium of legal stipulations designed to address cybersecurity vulnerabilities and penalize digital malfeasance. Notwithstanding this comprehensive statutory foundation, the research underscores a pronounced deficiency in the tangible execution and enforcement of these provisions. The study concludes that the Indonesian governance apparatus must proactively preempt cyber adversities through the meticulous formulation of robust cybersecurity strategies, entailing holistic defensive mechanisms, proportional counteractive measures, and a

*Corresponding author:
(Bayu Erlangga)

©2024 The Author(s).

This is an open-access article under CC-BY-SA license (<https://creativecommons.org/licence/by-sa/4.0/>)



fortified juridical order requisite for stringent governance of the nation's cyber terrain.

1. Introduction

The contemporary epoch, characterized by the pervasive integration of digital networks and advanced technological apparatuses, has fundamentally reconfigured the modalities of human interaction, commerce, and governance. Within this swiftly evolving milieu, the virtual domain, colloquially termed cyberspace, has transitioned from a novel communicative adjunct to an indispensable cornerstone of societal infrastructure. This interconnected sphere effectively dissolves conventional geographic demarcations, enabling instantaneous exchange and access across vast expanses (Ngo et al., 2020). However, this digital convergence has concurrently engendered a parallel universe wherein the architecture of connectivity is as susceptible to exploitation as it is conducive to innovation. The ascendancy of this boundless digital ecosystem has precipitated an alarming proliferation of cybercrime, a sophisticated genus of transgression that leverages information technology to perpetrate illicit activities ranging from financial fraud and data breaches to coordinated assaults on critical national infrastructure (Rajasekharaiah et al., 2020). As Indonesian society becomes increasingly enmeshed within this global digital lattice, the nation confronts a pressing imperative to not only legislate against these

emergent threats but to ensure the meticulous and efficacious implementation of such legal instruments through sound administrative praxis.

The exponential surge in internet utilization across the Indonesian archipelago has, regrettably, expanded the threat vector for malicious cyber actors who adeptly navigate and circumvent existing regulatory controls. The borderless nature of cyberspace complicates jurisdictional enforcement, allowing criminal enterprises to orchestrate attacks that transcend sovereign territories with relative impunity (Srivastava et al., 2020). In response to this escalating peril, the Indonesian government has instituted a strategic and systemic framework concerning cybersecurity, primarily orchestrated under the aegis of the Ministry of Communication and Informatics (MCI). This central coordinating body operates in concert with specialized technical units, including the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), the Directorate of Information Security, and the Information Security Coordination Team (Aulianisa & Indirwan, 2020; Rizal & Yani, 2016). Furthermore, the governance of cyber order is augmented by community-centric entities such as the Indonesia Academic Computer Security Incident Response Team (IDACAD-CSIRT) and the Indonesia Communication Emergency Response Team (ID-CERT), which function as auxiliary supports to the state apparatus in managing digital security crises (Rohman et al., 2022). The legislative cornerstone of this national effort is encapsulated within Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), supplemented by a constellation of ancillary regulations intended to fortify the digital perimeter (Safiranita et al., 2021).

Despite the existence of this multifaceted institutional and legislative architecture, a discernible chasm persists between the codified intent of the law and its tangible enforcement and administrative application. The mere promulgation of statutes does not ipso facto translate into a secure and resilient cyber ecosystem. The efficacy of Indonesia's cyber defense posture is contingent upon the robust execution of public administration duties, a domain where the principles of good governance, including transparency, accountability, and participatory engagement, must be meticulously applied. Non-governmental watchdogs, such as the Institute for Digital Law and Society (Tordillas), have meticulously documented the judicial disposition of cyber-related cases, revealing a preponderance of litigation centered on defamation, hate speech, and online blasphemy rather than sophisticated technical intrusions (Ibrohim & Budi, 2019; Marwan & Bonfigli, 2022). This jurisprudential trend intimates that while the legal framework is actively utilized, its application may be skewed towards content regulation rather than the comprehensive mitigation of systemic cyber vulnerabilities. From the vantage point of public administration, there exists an exigent necessity for a holistic and meticulously orchestrated governance model capable of steering governmental action toward optimal outcomes. The current operational landscape is marred by a deficit in the coherent implementation of foundational governance precepts, such as procedural propriety, human rights safeguards, and outcome-oriented effectiveness, thereby curtailing the state's capacity to mount a nimble and adequate rejoinder to the fluid dynamics of digital criminality (Marwan & Bonfigli, 2022).

This scholarly investigation is predicated upon two cardinal objectives. The primary aim is to delineate and critically appraise the juridical and regulatory scaffolding that governs cybercrime in Indonesia. The secondary aim is to ascertain and explicate the precise functional role of public administrative bodies in the ongoing endeavor to curtail and neutralize cyber malfeasance within the nation's digital frontiers. The timeliness and pertinence of this study are underscored by Indonesia's accelerating digital transformation, which paradoxically amplifies its exposure to a spectrum of cyber threats. A systematic inquiry into the interplay between legal formulation and administrative execution is indispensable for diagnosing the lacunae that undermine national cybersecurity resilience. The scholarly contribution of this research resides in its synthesis of doctrinal legal analysis with public administration theory, thereby generating novel insights into the operationalization of cyber statutes. Furthermore, the practical ramifications of this study extend to policymakers and enforcement agencies; the findings proffer actionable intelligence and prescriptive recommendations aimed at heightening societal cognizance regarding cyber perils and refining the procedural mechanisms through which cybersecurity legislation is operationalized to safeguard Indonesia's digital sovereignty.

2. Method

This scholarly inquiry adopts a qualitative research paradigm to interrogate the functional interplay between public administrative mechanisms and the legal infrastructure governing cybercrime mitigation in Indonesia. The selection of a

qualitative orientation is predicated upon the study's intrinsic objective to excavate nuanced understandings of regulatory efficacy and institutional conduct, rather than merely quantifying the frequency or typology of cyber infractions. The research is anchored within an interpretivist epistemological framework, which affords the latitude to engage in inductive reasoning and contextual interpretation of legal texts and policy instruments. This philosophical stance acknowledges that the meaning and operational significance of legal provisions are not static but are contingent upon the socio-political and administrative milieus within which they are embedded.

In terms of methodological architecture, the investigation employs a normative juridical approach, a conventional modality within legal scholarship that centers on the systematic examination of authoritative legal sources. Data acquisition was bifurcated into two distinct yet complementary streams: primary and secondary legal materials. The primary corpus encompasses a comprehensive array of binding juridical instruments, including statutory enactments, governmental regulations, presidential decrees, ministerial ordinances, and pertinent judicial decisions that constitute the formal architecture of Indonesia's cybersecurity and anti-cybercrime regime. Specific attention was directed toward foundational legislation such as Law No. 11 of 2008 on Electronic Information and Transactions, alongside its derivative implementing regulations and cognate statutes addressing telecommunications, public service delivery, national defense, and consumer protection.

Concurrently, the secondary data stream was curated through an extensive review of scholarly literature and jurisprudential commentary. This encompassed peer-reviewed journal articles, academic treatises, conference proceedings, and

analytical reports sourced from reputable digital repositories, including HeinOnline, Westlaw, LexisNexis, JSTOR, and Bloomberg Law. These secondary sources served to contextualize the primary legal materials within broader theoretical discourses on cyber governance, public administration efficacy, and comparative regulatory frameworks. The analytical procedure undertaken was governed by the principles of qualitative content analysis, a rigorous technique employed to distill, categorize, and interpret the latent themes, conceptual relationships, and terminological significations embedded within the assembled textual corpus (Campbell, 2020). Through this methodical interrogation of legislative language and policy articulation, the study endeavors to delineate the congruities and disjunctures between Indonesia's statutory aspirations and the administrative realities of cybercrime enforcement.

3. Results and Discussion

3.1 Institutional Architecture and Administrative Governance of Cyber Offenses in Indonesia

The Indonesian governmental apparatus, in concert with its affiliated public sector entities, has undertaken deliberate measures to erect a systemic framework for the stewardship of cybersecurity and the suppression of digital criminality. At the apex of this institutional edifice resides the Ministry of Communication and Informatics (MCI), which discharges the mandate of orchestrating and harmonizing national policy directives pertaining to the security of cyberspace. This ministerial coordination is not exercised in isolation; rather, it is buttressed by a triumvirate of

specialized governmental agencies vested with discrete operational responsibilities. These comprise the Information Security Coordination Team (ISCT), the Directorate of Information Security (DIS), and the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). The ISCT, inaugurated in April 2010, was conceived as a strategic initiative to cultivate expertise and propagate best practices in information technology security, thereby advancing the national agenda of cybercrime abatement. Concurrently, the DIS assumes custodianship over the formulation, implementation, and evaluative oversight of policies germane to information security governance, encompassing functions such as continuous monitoring, capacity-building through training, and comprehensive reporting mechanisms (Yulianto, 2021). The ID-SIRTII, established pursuant to Minister of Communication and Informatics Regulation No. 8 of 2012, is specifically tasked with the remediation of security exigencies affecting the nation's internet infrastructure backbone.

Beyond the purview of strictly governmental organs, the Indonesian cybersecurity ecosystem is augmented by the contributory endeavors of two community-based organizations that operate in a provisional yet substantively supportive capacity. The Indonesia Communication Emergency Response Team (ID-CERT) functions as a pivotal nexus, collaborating synergistically with administrative authorities during exigent circumstances to foster the maturation and resilience of the nation's cyber defense posture. In a parallel vein, ID-CERT actively serves as a force multiplier for agencies such as ID-SIRTII, extending the operational reach and technical acumen available to state actors. Complementing this is the

Indonesia Academic Computer Security Incident Response Team (ID-ACAD-CSIRT), an consortium that aggregates the cybersecurity capabilities resident within Indonesian institutions of higher learning. This academic alliance is expressly oriented toward the promotion of preventative security protocols and the cultivation of a security-conscious ethos within the educational sector. Presently, the ID-ACAD-CSIRT network encompasses approximately forty member institutions, each affiliated with the broader CSIRT academic community (Yulianto, 2021).

Notwithstanding the existence of this ostensibly coherent institutional matrix, the operationalization of cybercrime governance in Indonesia is frequently characterized by fragmentation and a conspicuous absence of synergistic harmonization. The delineation of authority and the coordination of inter-agency responses remain suboptimal, resulting in a landscape where cybersecurity initiatives are often pursued in sectoral silos rather than as components of an integrated national strategy. This disaggregated approach engenders inefficiencies and redundancies, as disparate entities may pursue overlapping objectives without the benefit of a unified command or a standardized operational doctrine. The consequence is a cyber defense architecture that, while populated by competent individual units, lacks the cohesive resilience requisite to mount a coordinated rejoinder to sophisticated, multi-vector cyber onslaughts.

The lacuna in centralized, authoritative coordination is particularly pronounced when juxtaposed against the escalating sophistication and transboundary nature of contemporary cyber threats. Without a designated institution endowed with plenary authority to direct and synchronize the full

spectrum of cybersecurity operations, spanning prevention, detection, response, and recovery, the Indonesian governance framework remains susceptible to strategic incoherence. The current arrangement implies that the mantle of cybersecurity is diffused across multiple stakeholders, with the central government assuming a relatively circumscribed and at times reactive role in the overarching architecture of cyber defense. This diffusion of responsibility, while ostensibly promoting broad-based engagement, paradoxically dilutes accountability and impedes the expeditious decision-making that is indispensable during active cyber contingencies.

The efficacy of public administration in this domain is further attenuated by the persistent challenge of adapting bureaucratic processes to the velocity of technological change. Cybercriminals operate with alacrity, continually refining their modus operandi and exploiting emergent vulnerabilities with minimal latency. In contradistinction, the administrative machinery of the state, encumbered by hierarchical protocols, fiscal constraints, and the inherent inertia of large organizations, often struggles to match this tempo. This asymmetry between the agility of malefactors and the deliberative pace of administrative response constitutes a fundamental structural vulnerability within Indonesia's cybercrime governance paradigm. Addressing this disparity necessitates not merely the augmentation of technical capabilities but a fundamental re-engineering of administrative workflows and inter-agency collaboration protocols.

Furthermore, the existing framework evinces a discernible deficit in the systematic socialization and internalization of cybersecurity policies among relevant stakeholders. The mere promulgation of regulations and the establishment of

institutions do not, in themselves, guarantee operational efficacy. The translation of policy intent into tangible security outcomes is contingent upon the active engagement and capacitation of all actors within the ecosystem, including private sector entities, civil society organizations, and the general populace. The absence of robust mechanisms for disseminating awareness, fostering compliance, and incentivizing proactive security behaviors undermines the potential impact of even the most meticulously drafted legislative instruments. Consequently, the governance of cybercrime in Indonesia remains a work in progress, characterized by a promising institutional foundation that is yet to achieve its full potential due to persistent challenges in coordination, agility, and stakeholder mobilization.

3.2 Juridical Foundations and Legislative Instruments Governing Cyber Malefaction in Indonesia

The statutory framework underpinning Indonesia's efforts to combat cybercrime is anchored in a constellation of legislative enactments, the preeminent among which is Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law). This seminal piece of legislation constitutes the bedrock upon which subsequent regulatory edifice and policy directives pertaining to cybersecurity have been erected (Ardiansyah et al., 2022). The ITE Law articulates a comprehensive schema for the governance of electronic information, the validation of digital transactions, and the proscription of a spectrum of cybernetic offenses. It serves as the primary juridical reference point for adjudicating disputes and prosecuting infractions within Indonesia's digital domain. However, the ITE Law does not operate in a vacuum; its efficacy and scope are augmented and

circumscribed by a panoply of ancillary statutes that address intersecting dimensions of national security, public service delivery, and consumer welfare.

Among the salient legislative instruments that collectively constitute Indonesia's cybersecurity jurisprudential matrix is Law No. 25 of 2009 on Public Service. This statute imposes affirmative obligations upon governmental bodies to ensure the integrity, reliability, and security of electronic service delivery mechanisms (Mustafa et al., 2020). In an era where citizen-state interactions are increasingly mediated through digital platforms, the security of these conduits assumes paramount importance. Breaches in public service information systems not only erode citizen trust but may also precipitate tangible harms ranging from identity theft to the disruption of essential services. Consequently, the public service law provides an indirect yet potent legal basis for mandating robust cybersecurity measures within the administrative apparatus.

The national security dimension of cyberspace is addressed through a suite of laws that collectively articulate the state's prerogative and duty to defend its sovereign interests in the digital sphere. Law No. 3 of 2002 on State Defense establishes the foundational principle that the preservation of national sovereignty extends to all domains, including the virtual realm (Junaidi & Prakoso, 2021). This is complemented by Law No. 34 of 2004 on the Indonesian National Armed Forces, which delineates the role of the military in safeguarding the nation's territorial integrity against a spectrum of threats, including those emanating from or mediated through cyberspace (Gunawan, 2020). Furthermore, Law No. 2 of 2002 on the Indonesian State Police provides the juridical mandate for law enforcement agencies

to investigate and interdict cybercriminal activities (Sitompul & Hasibuan, 2021). The legislative landscape is further complicated by the inclusion of Law No. 15 of 2003 on the Eradication of Criminal Acts of Terrorism, which superseded Government Regulation in Lieu of Law No. 1 of 2002. This statute is increasingly pertinent in an age where terrorist networks exploit encrypted digital channels for recruitment, propaganda dissemination, and operational coordination.

Consumer protection in the digital marketplace is enshrined within Law No. 8 of 1999 on Consumer Protection. This legislation proffers legal recourse and safeguards for individuals who suffer pecuniary or other damages as a consequence of fraudulent or negligent conduct in electronic commerce (Atikah, 2020). As Indonesia's digital economy burgeons, the salience of this statutory protection escalates commensurately. Consumers transacting on e-commerce platforms, utilizing digital financial services, or engaging with online content providers are exposed to a unique constellation of risks, including data theft, phishing scams, and fraudulent transactions. The consumer protection law provides a juridical avenue for aggrieved parties to seek redress, thereby indirectly incentivizing commercial entities to adopt stringent cybersecurity postures.

Notwithstanding the apparent breadth and depth of this legislative tapestry, scholarly scrutiny reveals critical deficiencies that attenuate its practical utility in the ongoing struggle against cyber malfeasance. A principal critique pertains to the generic and at times nebulous character of the statutory language. While the ITE Law and its cognate statutes delineate broad categories of prohibited conduct, they frequently lack the granular specificity required to effectively address the protean

and technologically intricate manifestations of contemporary cybercrime. This legislative ambiguity engenders interpretative challenges for law enforcement personnel, prosecutors, and the judiciary, potentially leading to inconsistent application and juridical uncertainty (Yulianto, 2021). The absence of precise technical definitions and clearly articulated evidentiary standards hampers the ability of the criminal justice system to mount effective prosecutions against sophisticated cyber adversaries.

Furthermore, the existing legal corpus is characterized by a conspicuous absence of specific normative provisions that comprehensively address the full spectrum of cybercriminal typologies. The law, as currently constituted, proscribes acts of unauthorized access, data interference, and system sabotage in broad strokes. However, it offers limited guidance on emergent phenomena such as ransomware deployment, cryptojacking, state-sponsored advanced persistent threats (APTs), or the weaponization of artificial intelligence for malicious purposes. This normative lacuna creates a juridical void that cybercriminals are well-positioned to exploit, operating with relative impunity in the interstices of an outdated or inadequately nuanced legal framework. The dynamic and continuously evolving nature of cyber threats renders static legislation perpetually vulnerable to obsolescence, underscoring the imperative for adaptive and future-oriented lawmaking.

The implementation of the ITE Law has also attracted considerable opprobrium due to perceived ambiguities and the potential for prosecutorial overreach. Critics have contended that certain provisions within the statute, particularly those pertaining to defamation and the dissemination of prohibited

content, are susceptible to instrumentalization for purposes extraneous to genuine cybercrime mitigation (Paterson, 2019). The elasticity of the statutory language has, in some instances, been exploited to curtail legitimate expression and to silence dissenting political voices, thereby transforming a legislative instrument ostensibly designed for cybersecurity into a mechanism of content control. This conflation of cybersecurity with content regulation not only diverts scarce enforcement resources from addressing genuine technical threats but also erodes public confidence in the legitimacy and impartiality of the legal framework governing cyberspace.

The regulatory ecosystem is further elaborated through subordinate instruments such as Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. This regulation provides technical specificity and operational guidance for the implementation of the broader principles articulated within the ITE Law. It addresses matters such as the certification of electronic systems, the security obligations of electronic system operators, and the procedures for cross-border data flows. Additionally, the government has promulgated a National Cybersecurity Framework intended to provide strategic direction and foster legal certainty for the expansion of the digital economy. However, the existence of these regulatory and policy instruments has not fully remedied the fundamental challenge of ensuring coherent and consistent implementation across the vast and decentralized Indonesian governance landscape. The absence of standardized documentation and harmonized operational procedures across all ministries and agencies continues to impede the seamless

execution of cybersecurity mandates, leaving the nation's digital infrastructure in a state of persistent vulnerability.

3.3 Impediments and Prospective Pathways in the Administrative Mitigation of Cyber Threats

The administrative apparatus charged with the stewardship of Indonesia's cybersecurity and the interdiction of cybercrime confronts a formidable array of impediments that collectively undermine the efficacy of its endeavors. A primary and perennially vexing challenge resides in the exponential velocity of technological advancement, which consistently outstrips the adaptive capacity of bureaucratic institutions. The digital ecosystem is characterized by ceaseless innovation, with novel platforms, applications, and protocols emerging in rapid succession. While this technological dynamism fuels economic growth and societal connectivity, it simultaneously expands the attack surface available to cybercriminals and engenders legal and administrative quandaries for which existing frameworks offer inadequate guidance (Epafra et al., 2019; Widiyari & Thalib, 2022). The proliferation of disinformation and the concomitant rise in cases of digital blasphemy exemplify the unanticipated societal externalities of unfettered digital connectivity, posing challenges that transcend purely technical cybersecurity concerns and implicate broader questions of social cohesion and legal pluralism.

The chronic deficit in threat intelligence constitutes a further critical vulnerability within Indonesia's administrative response to cybercrime. Effective cybersecurity posture is predicated upon the timely acquisition, analysis, and dissemination of actionable intelligence regarding emergent threats, adversary

tactics, and system vulnerabilities. However, public sector entities in Indonesia are often encumbered by a paucity of sophisticated threat intelligence capabilities, a challenge compounded by the sheer volume of data generated within digital networks, legitimate concerns regarding privacy and legal compliance, and the variable quality of available threat data (Abu et al., 2018). The inability to distinguish signal from noise in the vast ocean of digital exhaust leaves administrators ill-equipped to prioritize resources, anticipate attacks, or mount proactive defenses. This intelligence deficit perpetuates a reactive posture, wherein administrative action is predominantly triggered post-incident rather than preemptively neutralizing threats before they materialize.

Compounding the technical and informational challenges is a pervasive and deeply entrenched lack of cybersecurity awareness across multiple strata of Indonesian society. This deficit in digital literacy and security consciousness renders the nation's cyberspace disproportionately susceptible to a wide array of threats, ranging from rudimentary phishing campaigns to more sophisticated social engineering exploits (Blin et al., 2022). Low levels of awareness correlate directly with suboptimal adoption and utilization of protective software, weak password hygiene, and a general insouciance toward the security implications of online behavior. This widespread vulnerability among the general populace not only facilitates individual victimization but also creates vectors through which malicious actors can compromise larger institutional networks. The government's capacity to respond effectively to cybercrime is thus inextricably linked to its success in elevating

public consciousness and fostering a culture of collective cyber hygiene through sustained educational and awareness-raising initiatives (Srinivas et al., 2019).

The juridical landscape itself constitutes a significant impediment to effective administrative action. The extant cybercrime legislation has been the subject of sustained critique for its perceived inadequacy, inconsistency, and susceptibility to interpretative ambiguity. The rapid digitalization of Indonesian society has not been matched by a commensurate evolution in the sophistication or coherence of its cyber laws (Mahrina et al., 2023). Although the Electronic Information and Transactions Law underwent amendment in 2016, it continues to attract censure for its vagueness and the potential for its provisions to be wielded as instruments of political expediency rather than as shields against genuine cyber threats (Paterson, 2019). This juridical uncertainty creates a chilling effect on innovation and complicates the efforts of law enforcement and administrative agencies to operate with the clarity and confidence requisite for effective intervention. Malefactors and corrupt officials are adept at exploiting the interstices and ambiguities within the legal framework, thereby further complicating the task of governance.

Fiscal constraints represent an additional and often decisive barrier to the realization of robust cybercrime governance. The administration of a comprehensive national cybersecurity program is an inherently resource-intensive undertaking, necessitating substantial investments in advanced technological tools, specialized human capital, and ongoing operational expenditures (Nugraha & Putri, 2016). Budgetary limitations frequently compel public sector entities to make invidious trade-offs, prioritizing certain functions while neglecting others that may be equally

critical to long-term resilience. The inability to procure cutting-edge forensic equipment, to recruit and retain top-tier cybersecurity talent, or to fund continuous professional development for existing personnel erodes the state's capacity to prevent, detect, and investigate cybercrime with the requisite degree of technical proficiency (Peters & Jordan, 2019). This resource scarcity is particularly acute in the context of a developing economy, where cybersecurity must compete for finite public funds against a panoply of other pressing social and infrastructural demands.

The absence of a comprehensive and harmonized personal data protection regime further exacerbates the challenges confronting public administration. Indonesia's legal landscape regarding personal data is currently characterized by a fragmented patchwork of provisions scattered across various sectoral statutes, engendering confusion and juridical ambiguity that cybercriminals are quick to exploit (Paterson, 2019). The lack of a unified and robust data protection law undermines the trust that citizens and businesses place in digital ecosystems and complicates the efforts of law enforcement agencies to investigate and prosecute data-centric crimes. The anticipated enactment of comprehensive data protection legislation is widely viewed as an indispensable step toward rectifying this deficiency and bringing Indonesia's regulatory environment into closer alignment with international best practices.

The potential for synergistic collaboration between the public and private sectors represents a largely untapped reservoir of capability in the fight against cybercrime. Private enterprises, particularly those in the technology, finance, and telecommunications sectors, possess substantial technical expertise, threat

intelligence, and infrastructural resources that could significantly augment the state's capacity to detect and respond to cyber threats (Boes & Leukfeldt, 2017). However, the realization of this potential is contingent upon the establishment of clear legal guidelines and governance frameworks that delineate the modalities of public-private partnership while safeguarding the rights and privacy of customers and citizens (Saputra et al., 2019). The current regulatory environment, as articulated in instruments such as Presidential Regulation No. 53 of 2017 and its subsequent amendment, Presidential Regulation No. 133 of 2017, implicitly acknowledges the importance of multi-stakeholder engagement in the formulation of a national cybersecurity framework. Nevertheless, the translation of this aspirational principle into concrete, operational collaboration is hampered by a persistent lack of trust, inadequate coordination mechanisms, and the absence of formalized protocols for information sharing and joint incident response.

To surmount these multifarious impediments, a concerted and multifaceted response is imperative. The Indonesian government must transcend the limitations of its current reactive posture and embrace a proactive, strategic orientation toward cybersecurity. This entails not only the amendment of relevant statutory provisions to enhance specificity and address emergent threat vectors but also the cultivation of a robust institutional culture of cybersecurity within all echelons of public administration. The experience of neighboring ASEAN member states, such as Malaysia and Singapore, which have successfully instituted specialized agencies and promulgated specific, actionable cybersecurity policies tailored to their respective threat landscapes, offers instructive precedents (Sunkpho et al., 2018). Whether

through the establishment of a dedicated cyber authority or the unambiguous designation of an existing institution as a segment leader with overarching coordinating powers, Indonesia must move decisively to remedy the current diffusion of responsibility and establish a clear locus of accountability for national cybersecurity. The alternative is to remain in a state of perpetual vulnerability, wherein the nation's digital defenses are perpetually a step behind the ingenuity and malice of its cyber adversaries.

4. Conclusion

This investigation has critically examined the functional role of public administration in mitigating cybercrime within Indonesia, juxtaposed against the nation's extant legal and regulatory frameworks. The analysis reveals a discernible paradox: Indonesia possesses a relatively comprehensive corpus of legislative instruments and institutional mechanisms, yet their operational efficacy remains significantly attenuated. The primary impediments identified include juridical ambiguity within statutory provisions, fragmented inter-agency coordination, a chronic deficit in specialized threat intelligence, and pervasive cybersecurity unawareness among the populace. Consequently, the mere existence of laws does not ipso facto translate into resilient cyber defenses. The administrative apparatus must transcend its current reactive posture and address the systemic lacunae that undermine the translation of legislative intent into tangible security outcomes.

To fortify Indonesia's digital sovereignty, a strategic recalibration of governance is imperative. This necessitates the refinement of ambiguous statutory

language to encompass emergent cybercriminal typologies and the unambiguous designation of a centralized coordinating authority to rectify institutional fragmentation. Furthermore, the cultivation of robust public-private partnerships is essential for harnessing sectoral expertise and intelligence. Without such concerted reforms, Indonesia's digital infrastructure will remain perennially vulnerable. The government must therefore transition from a diffused, reactive stance toward a proactive, integrated, and adaptive governance model that prioritizes accountability, transparency, and the rigorous execution of cybersecurity mandates.

References

- Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence: Challenges and opportunities. *Journal of Advanced Research in Computing and Applications*, 13(1), 1–8.
- American Concrete Institute. (2011). Concrete quality, mixing, and placing. In *Building code requirements for structural concrete (ACI 318M-11) and commentary* (pp. 65–82). American Concrete Institute.
- Anjani, N. H. (2021). *Cybersecurity protection in Indonesia* [Policy brief]. Center for Indonesian Policy Studies.
- Ardiansyah, A., Rafi, M., & Amri, P. (2022). The importance of strengthening legal concepts in overcoming cybercrime during the COVID-19 pandemic in Indonesia. In *HCI for cybersecurity, privacy and trust: 4th International Conference*,

- HCI-CPT 2022* (pp. 469–479). Springer. https://doi.org/10.1007/978-3-031-05563-8_29
- Atikah, I. (2020). Consumer protection and fintech companies in Indonesia: Innovations and challenges of the Financial Services Authority. *Jurnal Hukum dan Peradilan*, 9(1), 132–153. <https://doi.org/10.25216/jhp.9.1.2020.132-153>
- Aulianisa, S. S., & Indirwan, I. (2020). Critical review of the urgency of strengthening the implementation of cyber security and resilience in Indonesia. *Lex Scientia Law Review*, 4(1), 31–45. <https://doi.org/10.15294/lesrev.v4i1.38197>
- Blin, P. F., Aditya, T., Claramunt, C., Kermarrec, Y., & Santosa, P. B. (2022). Cybersecurity risk-management to maintain integrity land data transactions: Application to Indonesian and French land administration systems. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 48, 29–31. <https://doi.org/10.5194/isprs-archives-XLVIII-4-W3-2022-29-2022>
- Boes, S., & Leukfeldt, E. R. (2017). Fighting cybercrime: A joint effort. In *Cyber-physical security: Protecting critical infrastructure* (pp. 185–203). Springer. https://doi.org/10.1007/978-3-319-32824-9_9
- Campbell, A. J. (2020). Let the data speak: Using rigour to extract vitality from qualitative data. *Electronic Journal of Business Research Methods*, 18(1), 1–15. <https://doi.org/10.34190/JBRM.18.1.001>
- Epafra, L. C., Kaunang, H. P., & Asri, S. (2019). Religious blasphemy and monitory society in Indonesian digital age. *Jurnal Kawistara*, 9(2), 220–230. <https://doi.org/10.22146/kawistara.41169>

- Farida, N., & Syaquillah, M. (2023). Ring of security review on the vital objects of the electricity subfield. *Jurnal Ekonomi*, 12(2), 1248–1258.
- Gunawan, S. (2020). The principle of control non-primary gun system of the Indonesian National Army protect soldiers. *BESTUUR*, 8(2), 152–164. <https://doi.org/10.20961/bestuur.v8i2.43140>
- Hartanto, D., Dalle, J., Akrim, A., & Anisah, H. U. (2021). Perceived effectiveness of e-governance as an underlying mechanism between good governance and public trust: A case of Indonesia. *Digital Policy, Regulation and Governance*, 23(6), 598–616. <https://doi.org/10.1108/DPRG-03-2021-0046>
- Ibrohim, M. O., & Budi, I. (2019). Multi-label hate speech and abusive language detection in Indonesian Twitter. In *Proceedings of the Third Workshop on Abusive Language Online* (pp. 46–57). Association for Computational Linguistics. <https://doi.org/10.18653/v1/W19-3506>
- Junaidi, M. E., & Prakoso, L. Y. (2021). Pancasila as the basis for Indonesia's universal defense. *Journal of Social and Political Sciences*, 4(2). <https://ssrn.com/abstract=3838453>
- Klenka, M. (2021). Aviation cyber security: Legal aspects of cyber threats. *Journal of Transportation Security*, 14(3–4), 177–195. <https://doi.org/10.1007/s12198-021-00232-8>
- Mahrina, M., Sasmito, J., & Zonyfar, C. (2023). The Electronic Information and Transactions Law (EIT Law) as the first cybercrime law in Indonesia: An introduction and its implementation. *Pena Justisia*, 21(2). <https://doi.org/10.31941/pj.v21i2.2680>

- Mangku, D. G. S., Yulianti, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The personal data protection of internet users in Indonesia. *Journal of Southwest Jiaotong University*, 56(1).
- Marwan, A., & Bonfigli, F. (2022). Detection of digital law issues and implication for good governance policy in Indonesia. *BESTUUR*, 10(1), 22–32. <https://doi.org/10.20961/bestuur.v10i1.59143>
- Mustafa, D., Farida, U., & Yusriadi, Y. (2020). The effectiveness of public services through e-government in Makassar City. *International Journal of Scientific & Technology Research*, 9(1), 1176–1178.
- Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, 45(4), 430–451. <https://doi.org/10.1177/0734016820934175>
- Nugraha, L. K., & Putri, D. A. (2016). *Mapping the cyber policy landscape: Indonesia*. Global Partners Digital.
- Onyshchenko, S., Bilko, S., Yanko, A., & Sivitska, S. (2023). Business information security. In *Proceedings of the 4th International Conference on Building Innovations: ICBI 2022* (pp. 769–778). Springer. https://doi.org/10.1007/978-3-031-17385-1_65
- Paterson, T. (2019). Indonesian cyberspace expansion: A double-edged sword. *Journal of Cyber Policy*, 4(2), 216–234. <https://doi.org/10.1080/23738871.2019.1627476>

- Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *Journal of National Security Law & Policy*, 10(3), 487–524.
- Putra, B. A. (2022). Cyber cooperation between Indonesia and the United States in addressing the threat of cyberterrorism in Indonesia. *International Journal of Multicultural and Multireligious Understanding*, 9(10), 22–33. <https://doi.org/10.18415/ijmmu.v9i10.4058>
- Rajasekharaiah, K., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. *IOP Conference Series: Materials Science and Engineering*, 981(2), Article 022062. <https://doi.org/10.1088/1757-899X/981/2/022062>
- Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, 4(1), 61–78. <https://doi.org/10.21512/jas.v4i1.967>
- Rohman, H., Sumarna, S., Suwanda, S., & Leksmanawati, W. (2022). Collaboration of ministries/institutions and the private sector in handling cyber threats through the establishment of Computer Security Incident Response Team (CSIRT). *Technium Social Sciences Journal*, 38, 87–102. <https://doi.org/10.47577/tssj.v38i1.7906>
- Safiranita, T., Waluyo, T. T. P., Calista, E., Ratu, D. P., & Ramli, A. M. (2021). The Indonesian Electronic Information and Transactions within Indonesia's broader legal regime: Urgency for amendment? *Jurnal HAM*, 12(3), 533–552. <https://doi.org/10.30641/ham.2021.12.533-552>

- Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's cyber security through public-private partnership (PPP). *Central European Journal of International and Security Studies*, 13(4), 104–120.
- Setiawan, A. (2019). National cybersecurity policy in the US and Indonesia. *UNTAG Law Review*, 3(1), 71–87. <https://doi.org/10.56444/ulrev.v3i1.1071>
- Sitompul, A., & Hasibuan, P. (2021). The morality of law enforcement agencies in money laundering with the origin of corruption. *European Science Review*, (9–10), 55–63. <https://doi.org/10.29013/ESR-21-9.10-55-63>
- Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178–188. <https://doi.org/10.1016/j.future.2018.09.063>
- Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: A cross-country study. *Journal of Global Information Technology Management*, 23(2), 112–137. <https://doi.org/10.1080/1097198X.2020.1752084>
- Su, Q., Wang, H., Sun, C., Li, B., & Li, J. (2022). Cyber-attacks against cyber-physical power systems security. *Applied Mathematics and Computation*, 413, Article 126639. <https://doi.org/10.1016/j.amc.2021.126639>
- Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity policy in ASEAN countries. In *17th Annual Security Conference* (pp. 1–7).

- Widiasari, N. K. N., & Thalib, E. F. (2022). The impact of information technology development on cybercrime rate in Indonesia. *Journal of Digital Law and Policy*, 1(2), 73–86. <https://doi.org/10.58982/jdlp.v1i2.165>
- Yulianto, A. (2021). Cybersecurity policy and its implementation in Indonesia. *Law Research Review Quarterly*, 7(1), 69–82. <https://doi.org/10.15294/lrrq.v7i1.43191>
- Yuswanto, A., Putrawan, I. M., & Eryanto, H. (2023). Cyber security strategy: Factors affecting performance at Security Operation Center (SOC) in Indonesia. *Res Militaris*, 13(1), 3110–3127.