International Journal of Cyber Operations and Cyber Security Governance
Volume 1 Issue 1, 2026

Examining Indonesia's Legislation on the Function of Public Administration in the Fight Against Cybercrime

Ashutosh Priya, Raj Joshi
[1,2]Research scholar
Department of Computer Engineering

Article Info
Received: 22-11-2025 Revised: 13-12-2025 Accepted: 08-02-2026 Published: 18-02-2026

Abstract
Cybercriminals are able to more readily break rules and regulations due to the proliferation of the Internet and technical advancements. This is why cybercrime is becoming a major problem in Indonesia very quickly. The fight against cybercrime is far from over, despite the abundance of literature, policy, and legal frameworks devoted to the subject. Through an examination of the relevant legislative framework, this research seeks to assess the role of Indonesia's public administration in the fight against cybercrime. The study's goal was accomplished via the use of a qualitative normative legal method. Information was culled from both main (publications, articles) and secondary (legal documents, statutes, case laws, etc.) sources. The research concluded that Indonesia's legislative frameworks, laws, and policies are well-equipped to detect and prevent cybercrime and security breaches. Unfortunately, cybercrime prevention and cybersecurity legislation are not being properly enforced. The Indonesian government must be proactive in preparing for cyber threats by creating robust cyber-security policies, outlining thorough measures to defend against cyber-attacks, quantifying the scope of these attacks, and determining the best ways to counter them. Additionally, the rule of law must be established to ensure that cyber-attacks in Indonesia are properly controlled.

Keywords: Cybercrime, Public Administration, Legal Framework, Indonesia

Introduction

Understanding the role of public administration, or good governance, in light of the changing nature of digital laws, the internet, and society is crucial (Hartanto et al., 2021). In this rapidly evolving age of globalisation and sophisticated technology, cyberspace has become indispensable since it bridges geographical gaps and brings people together in real time (Ngo et al., 2020). This new dimension, called "cyberspace," is perched above all wired computers. The rise of online, however, has heightened worries about cybercrime (Rajasekharaiah, Dule, & Sudarshan, 2020). The advent of such sophisticated commercial goods has spawned a new religion. Cyberdefense has therefore become an integral part of information technology (IT) strategies (Alhayani et al., 2021). Cyberspace not only endangers our nation's security, but also requires a thorough understanding of the rules and regulations set out by cyber law. According to Srivastava et al. (2020), cybercrime has the potential to impact countries and areas that are not physically located in the same country. Thus, in order to fight cybercrime, multilateral agreements are crucial on a global and national scale. Indonesian government organisations and official entities have established a plan and system for cyber security. Cyber security policy in Indonesia is coordinated by the "Ministry of Communication and Informatics (MCI)" (Yulianto, 2021). The Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), the Directorate of Information Security, and the Information Security Coordination Team are the three branches of the Indonesian government that are responsible for cyber defence (Aulianisa & Indirwan, 2020; Rizal & Yani, 2016). Furthermore, two community groups are active in cyber defence: "Indonesia Communication Emergency Response Team (ID-CERT)" and "Indonesia Academic Computer Security Incident Response Team

(IDACAD-CSIRT)" (Rohman et al., 2022; Yulianto, 2021). When it comes to enforcing national cyber law and security, these groups provide a hand to the government. The Indonesian government has developed a strategy for implementing cyber security in accordance with the "Indonesian Law No. 11 of 2008 on Electronic Information and Transaction (ITE)" (Safiranita et al., 2021). Many other policies are similar to this one. But these rules and regulations are only effective against cybercrime if enforced by the Indonesian government and other authorised public agencies. If cyber security regulations are to be properly enforced, the public administration should make a robust governance structure a top priority. A non-governmental organization in Indonesia called "The Institute for Digital Law and Society" is more often referred to as "Tordillas" (Marwan & Bonfigli, 2022). Jurisdictional rulings in Indonesian cases involving cybercrime have been studied by this group. According to research (Ibrohim & Budi, 2019; Marwan & Bonfigli, 2022), the most common types of cybercrime in the nation are prejudice, hate speech, and online defamation. Cybersecurity may be effectively regulated by public administrative institutions from the standpoint of good governance. Still, the government needs a system of good governance that is detailed, all-encompassing, and well planned so that it can respond effectively. There has been a failure on the part of Indonesian government agencies to adequately apply the principles of participation, accountability, efficacy, transparency, propriety, and human rights in the digital era, making it difficult to address the growing criminal trends and cybercrimes (2022).

There are two goals to this inquiry. Finding the cybercrime legislation in Indonesia is the primary goal. Finding out how the government of Indonesia combats cybercrime is the second goal. Given Indonesia's rising cybercrime rate and the need for an efficient cybersecurity system to address cyber concerns and crime, this research is of utmost importance to the nation. A number of theoretical and practical considerations are raised by the research, which adds to our understanding of the topic. Cybercrime assessment and monitoring is an essential part of the study's mission, and the government will be able to utilise the study's findings and recommendations to better educate the public and strengthen the enforcement of cyber security legislation in Indonesia.

Research Methodology

As this study seeks to examine the role of public administration in combating cybercrime in Indonesia and the legal framework of the Indonesian government in combating cybercrime, the qualitative research method has been employed. The qualitative research method is therefore appropriate for this investigation. In addition, the researcher has adopted interpretivism as a research philosophy because it employs an inductive methodology. In addition, the researcher has utilized a "standard legal research method" for this purpose. The information was gathered from both primary and secondary sources. For the primary data collection, the researcher has collected information from various primary legal sources, such as legal documents, statutes, and case laws. In addition, for the secondary data collection, the researcher gathered information from various sources, including journal articles, books, and online databases such as Hein Online, West Law, Lexis Nexis, JSTOR, Bloomberg Law, and other sources. This research employs a content analysis approach to analyze the data. Analyzing qualitative data, content analysis is a well-known technique. It is used to determine the presence of specific concepts, themes, or terms in a set of qualitative data (Campbell, 2020). Using this method of analysis, the researcher has analyzed and quantified the data and identified the presence of specific relationships and meanings of particular concepts, themes, and terms in the study's collected data set.

Literature Review

Indonesian Cybercrime Legislation

Cybersecurity is supported by many laws in Indonesia. According to Ardiansyah, Rafi, and Amri (2022), the principal cyber security legislation in Indonesia is legislation 11 of 2008, which deals with electronic information and transactions. Legislative bodies and the executive branch have codified a plethora of national cybersecurity policies in accordance

with existing legislation. Cybercrime security is also addressed by a variety of Indonesian laws, such as legislation number 25 of 2009 on public service, law number 34 of 2004 on Indonesian national military forces, and law number 15 of 2003 on criminal eradication and terrorism (Mustafa, Farida, & Yusriadi, 2020; Gunawan, 2020). The following laws have been superseded by this one: Law No. 1 of 2002 (Yulianto, 2021), Law No. 3 of 2002 (Junaidi & Prakoso, 2021), Law No. 2 of 2002 (Sitompul & Hasibuan, 2021), and Law No. 8 of 1999 (Atikah, 2020) pertaining to consumer protection in Indonesia. It is MCI's responsibility to enforce Indonesian security laws and regulations pertaining to cybercrime. To maximise the efficiency with which these rules and regulations were put into play, more details and resources on implementation tactics, as well as a suitable organisational and corporate model, were necessary.

Implementing Indonesia's national cyber defence also requires cross-institutional cooperation, according to the Republic of Indonesia's Ministry of Defence (Marwan & Bonfigli, 2022). Indonesia is fighting cybercrime, but it's a patchwork effort since there isn't proper coordination. Inadequate cybersecurity poses a significant threat to national security, since it has the potential to cripple a nation's vital infrastructure (Farida and Syauqillah, 2023). Soekarno-Hatta International Airport is one example. Numerous attacks regularly compromised and rendered unusable the airport's radar systems. Mangku et al. (2021) states that in order to govern all parts of cyber security in the area, Indonesia needs a comprehensive strategy. All procedures pertaining to information security and cybercrimes should be standardised and documented in accordance with applicable laws, rules, statutes, and regulations.
The function of government agencies in the fight against cybercrime
There is a cyber war going on, says Klenka (2021), and to stop it, every area needs strong cyber security rules and regulations that are put into place correctly. In order for Indonesia to participate in cyberwarfare, the country's infrastructure must be comprehensive and up to par with international norms (Putra, 2022). A defence perimeter and a comprehensive mechanism for monitoring the network are also necessary. A network security assessment system, control measures, and an information system to monitor network incidents quickly and appropriately are also necessary components of the country's information and communication technology (ICT) system, which is responsible for cyber policy and security. The secrecy, authenticity, and reliability of data stored online are crucial to the delivery of public services in this age of digitisation and globalisation (Onyshchenko et al., 2023). As a result, protecting the nation's cyberspace is crucial for maintaining national security. A national defence agency may feel the effects of a cyberattack firsthand, say Su et al. (2022). Therefore, it is critical to access and monitor cybercrimes for the sake of consumer safety and national security, not only for the sake of technical computer problems. There is still little evidence of a coordinated effort at the government level to strengthen Indonesia's cyber defences. Cybersecurity and the country's efforts to fight cybercrime are still quite sectoral, with each sector's resources and priorities playing a significant role.

In addition, according to Al-Qahtani and Cresci (2022), Indonesia's defence capabilities, countermeasures, and cyber security are weak and highly susceptible to large-scale assaults. Cybersecurity and cybercrime are not specifically addressed by Indonesia's laws and regulations, despite the fact that they do exist. Consequently, they are useless when put into practice; instead, the government and public administration should educate all relevant parties about them and take action to stem the tide of the rapidly increasing cybercrime in the nation.

Results and Discussion

Governance of Cybercrime in Indonesia

Indonesia's The government and official community of Indonesia have already established a cybersecurity plan and framework. When it comes to cybersecurity, Indonesia's policies are coordinated by the Ministry of Communication and Informatics, or MCI. In Indonesia, three government entities are responsible for cybersecurity: the "Information security coordination team" (ISCT), the "Directorate of Information Security" (DIS), and the reaction team of Indonesia security incidents involving internet infrastructure (ID-SIRTII). With an emphasis on IT practices and knowledge, ISCT was established in April 2010 to strengthen Indonesia's cyber defences and fight cybercrime. When it comes to information security governance, the DIS has taken care of the policy's task establishments, monitoring, training, evaluation, and reporting (Yulianto, 2021). In order to address safety issues connected to the internet infrastructure, the government adopted ID-SIRTII based on MOC "Minister of communication and informatics No.8 of 2012" rules. For the time being, two Indonesian community groups are working on cybersecurity. The Indonesian government's administration and the accountable institution known as "communication emergency response" work together in specific cases to advance the cause of "cyber security in Indonesia." And government entities like ID-SIRTII actively benefit from "ID-CERT" as a support sector. Universities in Indonesia are working to increase awareness of security threats and develop response plans via the "Academic computer security incident response team" (ID-ACAD-CSIRT). Forty individuals are now associated with ID-ACAD-CSIRT via CSIRT-affiliated educational institutions (GRALDI, 2022; Yulianto, 2021).

Legal Framework Related to Cybercrime in Indonesia

The Indonesian government has incorporated a procedure based on the implementation of cyber security into the "Electronic Information and Transaction (ITE) Law No.11 of 2008" Numerous laws are indirectly associated with the strategy, including "Law no. 36 of 1999 regarding Telecommunication and Law no.14 of 2008" regarding the directness of public data (American Concrete Institute, 2011). In addition, the following Indonesian laws support the application of cybersecurity to combat cybercrime:

1. Consumer Protection Law No. 8 of 1999.
2. The Republic of Indonesia and state police Law No. 2 of 2002
3. State Defense Law No. 3 of 2002.
4. Instead of Law No. 1 of 2002, enactment of government regulations on terrorism and crime eradication as a law (Law No. 15 of 2003).
5. Indonesian National Armed Forces (Law No.34 of 2004).
6. Public Service Law No. 25 of 2009.

Current Policy of Cyber Security to Prevent cyber-crime in Indonesia

In 2007, The regulations concerning the use of telecommunication networks based on the Internet Protocol (IP) were released by the "Minister of Communication and Informatics" (MOC) and informatics in 2007 (later superseded by "No. 26/PER/M.Kominfo/5/2007"), laying the groundwork for Indonesia's cyber security policy and procedures. Cybercrime management in Indonesia is inadequate, incomplete, and fragmented due to the lack of standardised norms. It is a very dangerous condition since cyberattacks may cripple any nation's critical infrastructure. The "radar system of Soekarno-Hatta International Airport" has apparently collapsed on more than one occasion. Damage to a country's vital infrastructure due to cyberattacks is inevitable and almost usually illegal. Hence, Indonesia needs a system that keeps tabs on all the important parts of cybersecurity in a coordinated manner. The utilised communication includes all the rules that need a document as proof to carry out all procedures pertaining to information security, and it is a sequential policy that governs the ICT system. Consequently, in order to prevent being susceptible to a cyber war, infrastructure security must be in line with international norms. According to Aferudin and Ramli (2022) and Yuswanto, Putrawan, and Eryanto (2023), a network monitoring system and a perimeter defence that is well monitored are necessary. Further, an information and event management system is required to oversee security incidents in

order to implement the rules that are required to control the ICT system. In order to regulate and assess security, system safety evaluations are also required. The cybersecurity regulations in Indonesia are overseen and controlled by several laws and regulations, including "Law No. 11 of 2008" concerning electronic information and transactions, "Government Regulation No. 82 of 2012" concerning the implementation of digital systems and transactions, and various ministerial and governmental circular laws and regulations. The "government enacted the cyber-security National Framework." This comes after the introduction of cyber-security laws to guarantee the legitimacy of growth. But there are still holes in Indonesia's cybercrime legislation that need to be filled. No legislation in Indonesia defines or encompasses cybercrime since the law forbids all types of attacks, threats, misconduct, and exposure of sensitive information (Yulianto, 2021). Because cybercrime is ever-changing, it is crucial for law enforcement to stay ahead of the game.

Obstacles and challenges faced by public administration in combating cybercrime in Indonesia

All members of the community now have easy access to the ever-expanding technology and information resources made possible by technological advancements. The public administration in Indonesia is facing new legal concerns and issues brought about by the exponential rise of information technology (Epafras, Kaunang, & Asri, 2019; Widiasari & Thalib, 2022). There has been a rise in blasphemy cases in Indonesia due to the spread of false information caused by digital connection. Furthermore, cybercriminals are always coming up with new methods, and the government is slow to react and put rules into action. Problems with threat intelligence, such as data overload, privacy and legal issues, and poor threat data quality, make it hard for public administration to adjust to the evolving dynamics of the digital realm (Abu et al., 2018). A lack of cyber security awareness and sufficient cyber laws leads to inefficient public administration. Due to a lack of knowledge about cyber security, Indonesian cyberspace is open to attacks (Blin et al., 2022). Few people utilise protection software since they aren't aware of the risks. Education and awareness-raising may make cybercrime even more difficult to react to, therefore the government has to be ready (Srinivas, Das, & Kumar, 2019). Furthermore, online laws have been deemed insufficient and unsuitable. The lack of cybercrime laws allows criminals and corrupt authorities to engage in cybercrime (Paterson, 2019). This presents the government with an additional obstacle. Mahrina, Sasmito, and Zonyfar (2023) note that Indonesia's fast digital expansion has been accompanied by inadequate cyber security and inconsistent regulation. Electronic Information and Transactions Law (ITE) amendments were not made by Indonesia until 2016. However, others also argue that the ITE is too broad and ambiguous. The possibility of using ITE to "criminalise speech and silence political opponents" has been raised (Paterson, 2019).

Despite the government's best efforts, cybercrime remains a significant problem in Indonesia, and efforts to address it have been slow. Financial limitations have made it harder to combat cybercrime (Nugraha & Putri, 2016). The government is unable to engage in cutting-edge technology resources and experts in investigation and prevention because of financial and budgetary limitations (Peters & Jordan, 2019). Another problem with fighting cybercrime is the lack of data protection legislation. Criminals in Indonesia find it easier to perpetrate cybercrimes due to the uncertainty and confusion caused by the country's patchwork of personal data regulations (Paterson, 2019).

When it comes to combating cybercrime, collaboration between the public and commercial sectors might be vital (Boes & Leukfeldt, 2017). The problem, according to Saputra et al. (2019), is that there are no regulations outlining how public-private partnerships might aid law enforcement without infringing on customers' privacy and rights. The idea of incorporating all stakeholders, including the business sector, in the construction of a national cybersecurity framework is implicitly expressed in "Presidential Regulation No. 53 of 2017," which was later updated by "Presidential Regulation No. 133 of 2017"

(Saputra et al., 2019). But Indonesia can't handle cybercrime well since the public and commercial sectors don't work together (Saputra et al., 2019).

Conclusion

Within the context of Indonesia's current legislative frameworks, this research sought to examine the role of public administration in the fight against cybercrime. A thorough examination of Indonesia's cybercrime and cybersecurity laws revealed that the nation has mechanisms in place to control the latter. Having said that, the policies are vague and unspecific. According to Anjani (2021) and Setiyawan (2019), cyber security measures in Indonesia are inefficient because of weak regulations and inadequate execution. If Indonesia is serious about improving its cyber defences, its government or other authority bodies will need to pass new legislation or revise existing ones. The government of Indonesia has to take cyber security more seriously if it wants to stop cyberattacks. According to Sunkpho, Ramjan, and Ottamakorn (2018), some ASEAN states, including Malaysia and Singapore, have effectively addressed cyber threats by implementing targeted cybersecurity policies. Conversely, no agency in Indonesia has the power to handle and oversee cyber defences at this time. The Indonesian government has the power to designate any organization or structure as a sector leader, regardless of whether it is a specialised institution or not. This points to pervasive cybersecurity implementation and a low level of involvement from the Indonesian government in cyber defence. Some people try to break the law, control physical property and data, and breach rules all for their own financial and non-financial gain. Given this, the Indonesian government has to step up its efforts to protect the country's cyber defences from hackers and to prevent cybercrimes and assaults.

References

Published in 2018 by Abu, M. S., Selamat, S. R., Ariffin, A., and Yusof, R. Cyber threat intelligence–issue and problems. Volume 10, Issue 1, Pages 371-379, Indonesian Journal of Electrical Engineering and Computer Science. This publication is available online at this URL: https://doi.org/10.11591/ijeecs.v10.i.1. Aferudin, pp. 371–379 K., & F. Ramli (2022). The Indonesian National Critical Information Infrastructure Cybersecurity Information Sharing Framework Development. Journal of the Budapest International Research and Critics Institute (BIRCI-Journal), volume 5, issue 3, pages 22859-22872. This is the link to the paper by Al-Qahtani and Cresci (2022): https://bircu-journal.com/index.php/birci/article/view/6297. A review of phishing attempts and their responses during the COVID-19 pandemic: the COVID-19 scamdemic. The work of Alhayani, B., Abbas, S. T., Khutar, D. Z., and Mohammed, H. J. (2021) may be found at https://doi.org/10.1049/ise2.12073. Intelligent computation's best defences against cyber threats. Proceedings of Materials Today, 26–31. Publication by the American Concrete Institute; DOI: 10.1016/j.matpr.2021.02.557. in the year 2011. Concrete Quality, Mixing, and Placing. Sections 65-82 of the ACI 318M-11 Building Code Requirements for Structural Concrete and the Commentary thereto. Concrete Institute of America. Anjani, here is the link to the preview: https://www.concrete.org/Portals/0/Files/PDF/Previews/318-11_preview.pdf In 2021, N. H. A Framework for Indonesian Cybersecurity. Jakarta: CIPS, the Center for Indonesian Policy Studies. the authors of the article "CIPS-PB09.pdf" are Ardansyah and Amri (2022). The COVID-19 Pandemic in Indonesia and the Need to Reinforce Legal Concepts for Cybercrime Prevention and Oversight. Volume 24, Issue 1, Pages 469–479, Proceedings of the 2022 International Conference on Human-Computer Interaction (HCI-CPT), Part of the 24th HCI International Conference (HCII) Virtual Event, June 26–July 1, 2022. Atikah, I. (2020). Springer. https://doi.org/10.1007/978-3-031-05563-8_29. Concerning consumer safety and Indonesian financial technology businesses, the Financial Services Authority has been facing difficulties and innovations. Published in

the Jurnal Hukum dan Peradilan, volume 9, issue 1, pages 132-153. The output is a document with the DOI number 10.25216/jhp.9.1.2020.132-153.Linarisa and Indirwan published a work in 2020. Evaluate Critically the Critical Need to Strengthen Cyber Security and Resilience in Indonesia. Law Review of Lex Scientia, 4(1), pp. 31–45. The sentence might be paraphrased as: "Blin, In a recent publication by P. F. Aditya, T. Claramunt, Y. Kermarrec, and P. B. Santosa (2022). Managing Cybersecurity Risks to Preserve Trust Transactions involving land data: their use in the land administration systems of France and Indonesia. Section 48 of the International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences contains articles numbered 29 to 31. This publication is available online at: https://doi.org/10.5194/isprs-archives-XLVIII-4-W3-2022-29-2022.

In 2017, Boes and Leukfeldt published their work. Combating Cybercrime: How We Can Work Together. Pp. 185–203 in Cyber-Physical Security: Safeguarding Vital Infrastructure. Heidelberg: Springer, Cham. In 2020, Campbell published a work with the DOI 10.1007/978-3-319-32824-9_9. Listen to the numbers: How to glean life from qualitative data by using rigorous analysis. Article published in the Electronic Journal of Business Research Methods, volume 18, issue 1, pages 1–15, with the DOI number 10.34190/JBRM.18.1.001. Publisher: EThe relationship between religious blasphemy and Malaysian culture in the modern digital era (Pafras, Kaunang, & Asri, 2019). Publication: Jurnal Kawistara, Volume 9, Issue 2, Pages 220–230. The work of Farida and Syauqillah (2023) may be found at this URL: https://doi.org/10.22146/kawistara.41169. Encircle of Safety Evaluation on Essential Goals of the Electrical Domain. (Jurnal Ekonomi, 12(2), 1248-1258). Find the article at this URL: http://ejournal.seaninstitute.or.id/index.php/Ekonomi/article/view/1541.pdf.