The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia

by Ichsan Anwary

Submission date: 16-Jun-2023 12:24AM (UTC+0700)
Submission ID: 2116755452
File name: Final--Ichsan_IJCC_1.pdf (423.88K)
Word count: 6061
Character count: 37456

International Journal of Cyber Criminology
Vol 16 Issue 2 July – December 2022

The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia

Ichsan Anwary[1]
Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Abstract

With the expansion of Internet use and technological innovation, cybercriminals can now easily violate laws and regulations. Because of this, cybercrime-related issues are swiftly spreading throughout Indonesia. Even though there are numerous articles, policies, and legal frameworks to combat cybercrime, much work still needs to be done. This study aims to evaluate the function of public administration in combating cybercrime in Indonesia by analyzing the applicable legal framework. A qualitative normative legal approach was utilized in the research to achieve the study's objective. Data was gathered from primary (legal documents, legislations, laws, case laws, etc.) and secondary (publications, articles) sources. According to the findings, Indonesia has extensive policies, articles, and legal frameworks to inspect and control cyber security breaches and combat cybercrime. However, the formulated laws regarding cybersecurity and combating cybercrime are poorly implemented. The Indonesian government is obligated to anticipate cyber threats by adequately formulating cyber-security policies and identifying comprehensive steps for defending against cyber-attacks, their scale, and types of countermeasures, as well as developing the rule of law necessary to exert proper control over cyber-attacks in Indonesia.

Keywords: Cybercrime, Public Administration, Legal Framework, Indonesia

Introduction

It is essential to comprehend the evolution of digital laws, cyberspace, and society and the function of public administration, i.e., good governance (Hartanto et al., 2021). Cyberspace has become an integral part of human life in the swiftly transforming era of globalization and advanced technologies, as it connects individuals regardless of their distance (Ngo et al., 2020). This new universe, known as "cyberspace," exists on top of every computer system connected by a wire. With the advent of cyberspace, however, cybercrime concerns have increased (Rajasekharaiah, Dule, & Sudarshan, 2020). This advanced technology has given rise to a new consumerist cult. As a result,

[1] Faculty of Law, Universitas Lambung Mangkurat, Banjarmasin, Indonesia.
Email: ichsan.anwary@ulm.ac.id ORCID ID: https://orcid.org/0000-0002-4693-6467

the Internet and IT are now commonly used to combat cyber warfare (Alhayani et al., 2021). In addition to posing a threat to national security, there is an imperative need to comprehend the legal regulations imposed and implemented by cyber law. Cybercrime is a crime that can affect nations and regions beyond a country's geographical borders (Srivastava et al., 2020). Therefore, it is essential to have multilateral agreements at both the national and international levels to combat cybercrime.

Regarding cyber security in Indonesia, official bodies and government agencies have developed and implemented a strategy and system. In Indonesia, the "Ministry of Communication and Informatics (MCI)" coordinates cyber security policy (Yulianto, 2021). Indonesia's cyber security is handled by three government institutions: 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). Moreover, there are two community organizations involved in cyber security: "Indonesia Academic Computer Security Incident Response Team (IDACAD-CSIRT)" and "Indonesia Communication Emergency Response Team (ID-CERT)" (Rohman et al., 2022; Yulianto, 2021). These organizations assist the government in administering cyber security and cyber law and order within the nation. Based on the "Indonesian Law No. 11 of 2008 on Electronic Information and Transaction (ITE)", the Indonesian government has devised a cyber security implementation policy (Safiranita et al., 2021). There are numerous additional policies of this type.

Nonetheless, the public administration, government, and other authorized Indonesian departments/organizations/institutions must implement these policies and laws to combat cybercrime. The public administration should prioritize a good governance system to implement cyber security laws effectively. In Indonesia, "The Institute for Digital Law and Society" is a non-profit organization commonly known as "Tordillas" (Marwan & Bonfigli, 2022). This organization has analyzed the judgments and decisions made by Indonesian courts regarding cybercrime-related matters. It has been determined that bigotry, hate speech, and online defamation are the most prevalent cybercrimes in the country (Ibrohim & Budi, 2019; Marwan & Bonfigli, 2022). From the good governance perspective, public administrative entities may implement cyber security as an effective regulation. Nonetheless, there is a need for a thorough, comprehensive, and well-thought-out system of good governance that can assist and guide the government in acting most appropriately. To respond effectively to the rising criminal trends and cybercrimes in Indonesia, there is a lack of proper implementation of the principles of participation, accountability, effectiveness, transparency, propriety, and even human rights by government bodies in the digital age (Marwan & Bonfigli, 2022).

The present investigation has two objectives. The first objective is to identify Indonesia's cybercrime legal framework. The second objective is to determine the function of public administration in Indonesia's fight against cybercrime. This study is particularly essential in Indonesia, as the country is facing an increasing rate of cybercrime and requires a proper system to implement cybersecurity to combat cyber issues and cybercrime effectively. The study contributes new knowledge and insight into the subject and has several theoretical and practical implications. The study is important for assessing and monitoring cybercrimes, and it will also provide

the government with useful information and suggestions for raising awareness about cybercrimes and improving the implementation of cyber security laws for combating cybercrimes 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

Legal Framework of Cybercrime in Indonesia

Several laws in Indonesia support cyber security. Indonesian Law 11 of 2008 on electronic information and transaction is the primary cyber security law (Ardiansyah, Rafi, & Amri, 2022). Based on the law, the government and legislative entities have enacted numerous cybersecurity policies for the entire nation. In addition, several Indonesian laws support cybercrime security, including law number 25 of 2009 on public service (Mustafa, Farida, & Yusriadi, 2020), law number 34 of 2004 on Indonesian national armed forces (Gunawan, 2020), and law number 15 of 2003 on crime eradication and terrorism. This law replaces the regulation of law number one of 2002 (Yulianto, 2021), law number three of 2002 on state defense (Junaidi & Prakoso, 2021), law number two of 2002 on the Indonesian state police (Sitompul & Hasibuan, 2021), and law number eight of 1999 on consumer protection (Atikah, 2020). MCI implements cybercrime-related security laws and policies in Indonesia. However, the issued laws and regulations required additional elaborations and materials on implementation strategies and an appropriate organization and corporation model to optimize the implementation of these laws and policies.

Moreover, the Ministry of Defense of the Republic of Indonesia stated in 2013 that cross-institutional coordination is required to implement Indonesia's national cyber defense (Marwan & Bonfigli, 2022). Due to a lack of standard coordination, Indonesia's approach to combating cybercrime is partial, disorganized, and dispersed. According

to Farida and Syauqillah (2023), inadequate cybersecurity is extremely hazardous to national security because it can paralyze a state's critical infrastructure. Add the international Soekarno-Hatta Airport, for instance. Due to multiple intrusions, the airport's radar systems were repeatedly compromised and rendered inoperable. According to Mangku et al. (2021), Indonesia requires a comprehensive policy to regulate all aspects of cyber security in the region. There should be standard documentation in all laws, policies, legislation, and regulations that can guide the execution of all processes related to information and security and cybercrimes.

Role of Public Administration in combating cybercrime

According to Klenka (2021), there is a global cyber war, and to combat it, all regions must be active and vigilant and have strong and effective cyber security laws and policies that are properly implemented. For Indonesia to be able to engage in cyber warfare, Indonesia must have an infrastructure that conforms to international cyber war standards and is, therefore, comprehensive (Putra, 2022). In addition, a complete and effective network monitoring system and a defense perimeter are required. In addition, the ICT system that governs policy and cyber security in the country requires comprehensive event management and an information system to monitor incidents on the network promptly and appropriately, as well as control measures, security measures, and a network security assessment system. According to Onyshchenko et al. (2023), implementing public services in the era of digitalization and globalization is highly dependent on the confidentiality, integrity, and dependability of the information in cyberspace. Therefore, it is essential to guarantee a secure cyberspace, as this ensures the country's national security. According to Su et al. (2022), cyberattacks can directly impact national defense. As a result, accessing and monitoring cybercrimes as a matter of national security and consumer safety, as opposed to merely technical computer issues, is crucial. In Indonesia, implementing cyber defense has not yet emerged as a national collaborative initiative. Cyber security and the measures and initiatives taken to combat cybercrime in the country continue to be sectoral and highly dependent on the capabilities and interests of a specific sector.

Moreover Al-Qahtani and Cresci (2022), have argued that Indonesia's cyber security and defense countermeasures, deterrence, and capabilities are extremely vulnerable to massive cyberattacks and feeble. Even though Indonesia has some laws and policies for regulating cyber security and combating cybercrimes, these laws and policies are general and not specific. Therefore, their implementation is ineffective; hence, to make them effective, the government and public administration must socialize them with all stakeholders and control the country's swiftly growing cybercrimes.

Results and Discussion

Governance of Cybercrime in Indonesia

Indonesia's official community and government agencies have already implemented a cybersecurity strategy and system. The MCI (Ministry of Communication and Informatics) coordinates cybersecurity policies in Indonesia. ISCT's "Information security coordination team," DIS "Directorate of Information Security," and the response team of Indonesia security incident regarding internet infrastructure (ID-SIRTII) are the three government agencies involved in cybersecurity in Indonesia. ISCT was founded in April 2010 to

promote cyber security and combat cybercrime in Indonesia by concentrating on information technology practices and expertise. The DIS has addressed the policy's task establishments and their implementation, monitoring, training, evaluating, and reporting on information security governance (Yulianto, 2021). The government established ID-SIRTII based on MOC "Minister of communication and informatics No.8 of 2012" regulations to address internet infrastructure-related safety concerns.

In Indonesia, two community organizations are temporarily engaged in cybersecurity. Indonesia's communication emergency response is a responsible institution that collaborates with government administration in certain circumstances to promote the development of "cyber security in Indonesia." In addition, "ID-CERT" actively serves as a support sector for government agencies such as ID-SIRTII. The ID-ACAD-CSIRT "Academic computer security incident response team" emphasizes Indonesian universities seeking to promote security and preventative measures. Presently, 40 ID-ACAD-CSIRT members are affiliated with CSIRT academic 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 procedures and legal strategies for Indonesia's cyber security policy were initiated with the release of the "Minister of Communication and Informatics" "No. 26/PER/M.Kominfo/5/2007" regulations regarding the use of Internet Protocol-based telecommunication networks, which were later replaced by the regulations of MOC and informatics. As a result of the absence of harmonized standards, the management of cybercrime in Indonesia is insufficient and considered partial and dispersed. Cyberattacks have the potential to paralyze any nation's vital infrastructure, which makes it a very hazardous situation. For instance, multiple instances of the "radar system of Soekarno-Hatta International Airport" collapsing have been observed. Cyberattacks are always likely to cause undesirable and unlawful behavior to a nation's critical infrastructure. Therefore, Indonesia requires a procedure that supervises and monitors all relevant cybersecurity elements cohesively. Concerning the sequential policies by which the ICT system is governed, the used communication contains all the guidelines requiring a regular document as

evidence to conduct all information security-related processes. Therefore, infrastructure security must be aligned with international standards to avoid becoming vulnerable to a cyber conflict. Therefore, a network monitoring system and an adequately monitored perimeter defense are required (Aferudin & Ramli, 2022; Yuswanto, Putrawan, & Eryanto, 2023). In addition, the policies needed to govern the ICT system necessitate an event management and information system to monitor and administer security events. It also necessitates system safety evaluations through which security can be controlled and measured.

The context for cybersecurity regulations in Indonesia is monitored and governed by "Law No. 11 of 2008" regarding the transaction and electronic information, "Government Regulation No. 82 of 2012" regarding the application of digital transactions and systems, as well as ministerial and governmental circulatory minister and letter laws and regulations. In addition to initiating cyber-security legislation to assure legal conviction for expansion, the "government enacted the cyber-security National Framework." However, Indonesia's legal framework for combating cybercrime is still vulnerable and requires attention. As the law prohibits any form of attack, threat, malfeasance, or disclosure of confidential information, no law in Indonesia specifically normalizes and entails cybercrime (Yulianto, 2021). Cybercrime evolves persistently and continuously, making it essential for law enforcement to combat it.

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

Over the years, technology and information have expanded rapidly, and the development of technology has enabled all community members to have simple access. The rapid growth of information technology has created legal issues and challenges for Indonesia's public administration (Epafras, Kaunang, & Asri, 2019; Widiasari & Thalib, 2022). Digital connectivity has led to disinformation, resulting in an increase in blasphemy cases in Indonesia. In addition, cybercriminals are constantly developing new techniques, while the public sector remains sluggish in responding and implementing policies. Public administration confronts the difficulty of adapting to the changing dynamics of digital space due to a lack of threat intelligence, including data overload, privacy and legal concerns, and threat data quality (Abu et al., 2018). Ineffective public administration results from inadequate cyber legislation and cyber security consciousness. Low cyber security awareness makes Indonesia's cyberspace susceptible to threats (Blin et al., 2022). Lack of cyber security awareness results in low protection software adoption and use.

The government must be prepared to respond effectively to cybercrime, and education and awareness-raising can exacerbate the challenges (Srinivas, Das, & Kumar, 2019). In addition, cyberspace legislation has been criticized for being inadequate and insufficient. Criminals and corrupt officers exploit the absence of cybercrime legislation to indulge in cybercriminal activity (Paterson, 2019). This poses a further challenge for the government. Poor cyber security and inconsistent legislation have accompanied Indonesia's rapid digital growth (Mahrina, Sasmito, & Zonyfar, 2023). Indonesia did not amend the Electronic Information and Transactions Law (ITE) until 2016. Nonetheless, the ITE is also criticized for its ambiguity and

vagueness. It has been asserted that ITE can be utilized to "criminalize speech and silence political opponents" (Paterson, 2019).

Even though the Indonesian government intends to counteract cybercrime, progress has been sluggish due to an additional barrier. The administration of cybercrime has been hampered by budget constraints (Nugraha & Putri, 2016). Due to budgetary and financial constraints, the administration cannot invest in advanced technological tools and specialists for prevention and investigations (Peters & Jordan, 2019). The shortage of data protection laws is another obstacle to combating cybercrime. Diverse laws regarding personal data exist in Indonesia, resulting in confusion and ambiguity that makes it simpler for criminals to exploit the law and commit cybercrimes (Paterson, 2019).

Cooperation between the private sector and the government can be crucial in the fight against cybercrime (Boes & Leukfeldt, 2017). However, the lack of legal guidelines defining how public-private partnerships can assist law enforcement without jeopardizing the customer's rights and privacy presents a challenge (Saputra et al., 2019). In "Presidential Regulation No. 53 of 2017", which was subsequently amended by "Presidential Regulation No. 133 of 2017", the concept of involving all stakeholders, including the private sector, in the development of a national cybersecurity framework is implicitly conveyed (Saputra et al., 2019). However, a dearth of coordination between the public and private sectors hinders Indonesia's ability to manage cybercrime effectively (Saputra et al., 2019).

Conclusion

This study aimed to investigate the function of public administration in combating cybercrime in Indonesia in light of existing legal frameworks. After conducting an in-depth analysis of Indonesia's legal frameworks regarding cybercrime and cybersecurity, it was discovered that the country already has policies that regulate cyber-security. However, the policies are generic and lack specificity. Therefore, the application of cyber security in Indonesia is ineffective due to vulnerable policies, acts, or insufficient implementation, despite the existence of acts (Anjani, 2021; Setiyawan, 2019). The government or other authoritative entities must implement specific cybercrime control policies or amend relevant Articles to achieve effective cyber security results in Indonesia. To prevent cyberattacks, the Indonesian government must treat cyber security more seriously. Malaysia and Singapore, among other ASEAN members, have successfully contained and instituted specific cyber security policies in response to their potential threats (Sunkpho, Ramjan, & Ottamakorn, 2018).

On the other hand, Indonesia currently lacks any institution with unrestricted authority to deal with and manage cyber security. Even without a specialized institution, the Indonesian government can assign any institution or structure to become a segment leader. This suggests that the implementation of cybersecurity is widespread and that the Indonesian government plays a minor role in cyber defense. Some individuals violate legal norms, attempt to violate regulations, and control data security and physical property for their own (monetary and non-monetary) benefit. In light of this, the Indonesian government must make a concerted effort to anticipate cybercrimes and cyberattacks and to save the Indonesian cyber defense from cybercriminals.

Recommendations

In Indonesia, the number of cybercrimes is rising swiftly due to the public's increased internet use in their daily lives. Various parties, including government organizations, the private sector, law enforcement agencies, and the general public, are involved in the fight against cybercrimes. Therefore, the public administration can take into consideration the following recommendations to combat cybercrime, thereby promoting a safe environment for internet users and other stakeholders:

- The development of technologies and talents within law enforcement agencies must be considered if cybercrimes are to be reduced. The availability of advanced technologies to law enforcement agencies is crucial. Therefore, international cooperation can effectively acquire the necessary technologies and identify cyber threats with global implications.
- Promoting public awareness regarding cybercrimes can also effectively combat these crimes to safeguard the public and other associated stakeholders from such inadequate repercussions. Effective partnerships between the public and private sectors will exist for this purpose. This will facilitate effective knowledge sharing among the involved parties, creating effective strategies to combat cybercrime. Therefore, disseminating information can be an effective means of enhancing people's knowledge of cybercrimes. To achieve the desired results, cybercrime-specific online sharing platforms may be developed.
- The laws and regulations should be reevaluated based on the evolution of cybercrime. This can contribute to a global approach that reduces cybercrime. This will help maintain an up-to-date legal framework, supplying solutions to the problems associated with cybercrimes. In this regard, law enforcement agencies can contribute by actively and impartially reporting cybercrimes within the country. Consequently, the availability of a transparent report on cybercrimes will aid in formulating vital policies.

Research Implications

Theoretical Implications

With the continuous technological advancements of the modern world, the number of cybercrimes is rising rapidly; this has prompted the present research to concentrate on the legal framework of public administration in Indonesia in the context of cybercrimes. Consequently, this investigation is both theoretically and practically significant. Theoretically, this study has enhanced our comprehension of the function of public administration in cybercrimes. This study has also highlighted the role of various stakeholders in combating cybercrimes, including law enforcement agencies, governments, public sectors, private sectors, and civil society. In addition, this study has effectively determined the opportunities and obstacles the public sector faces in combating cybercrimes. However, the findings of this study can effectively encourage future research to concentrate on further categorizing cybercrimes according to the specificity of the associated offenses. This will contribute to a better comprehension of the legal implications of public administration about cybercrimes. This method will also enhance the value of the current study, making it an inspiration for future researchers. This study can also effectively affect how individuals perceive cybercrimes.

Practical Implications

In addition to its theoretical significance, this study includes practical implications contributing to its social value. This study, for instance, can effectively persuade governments to take significant steps to ensure the cyber security of residents. In addition, this study will effectively increase people's awareness of cybercrimes, encouraging them to report any online misbehavior they observe to the appropriate authorities. This will aid in the promotion of the whistleblowing procedure. In light of cybercrimes, the Indonesian government can enact significant policies and laws to protect the rights of whistleblowers. This will help promote social cohesion, leading to productive results. In addition, organizations can develop policies to ensure their employees' cyber security by providing them with password-protected and virus-free software. In addition, technological progress and innovation can be used to create and implement cybersecurity software that is difficult to infiltrate. However, this study has played a significant role in promoting social awareness of the insufficient consequences of cybercrimes. Important changes can also be made to cybercrime laws and regulations, focusing on protecting individuals.

Limitations and Future Research Recommendations

Every study has limitations, and this one is no exception. First, the study primarily employed a secondary data collection method because it relied on secondary sources and did not collect data directly from the respondents, such as the authorized and involved personnel, the authoritative persons who manage and administer cyber security laws and policies in the country, and the employees who work for these organizations or institutions. Second, the quantitative aspect of the study has been neglected in favor of qualitative research methods. Consequently, based on these limitations, the researcher has recommended that future researchers conduct surveys or interviews of the relevant target audience to conduct a preliminary study. It is also recommended that future researchers use a mixed-method approach in their studies to obtain a complete picture and an in-depth analysis of the role played by public administration in combating cybercrime in Indonesia and the legal framework of the Indonesian cybercrime regime.

References

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science, 10*(1), 371-379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Aferudin, F., & Ramli, K. (2022). The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 5*(3), 22859-22872. https://bircu-journal.com/index.php/birci/article/view/6297

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET Information Security, 16*(5), 324-345. https://doi.org/10.1049/ise2.12073

Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. *Materials Today: Proceedings*, 26-31. https://doi.org/10.1016/j.matpr.2021.02.557

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. https://www.concrete.org/Portals/0/Files/PDF/Previews/318-11_preview.pdf

Anjani, N. H. (2021). *Cybersecurity Protection in Indonesia*. Center for Indonesian Policy Studies (CIPS), Jakarta. https://www.econstor.eu/bitstream/10419/249442/1/CIPS-PB09.pdf

Ardiansyah, 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, Held as Part of the 24th HCI International Conference, HCII 2022, Virtual Event, June 26 – July 1, 2022, Proceedings* (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. http://dx.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 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, Cham. 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

Epafras, 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., & Syauqillah, M. (2023). Ring of Security Review on the Vital Objects of the Electricity Subfield. *Jurnal Ekonomi, 12*(2), 1248-1258. http://ejournal.seaninstitute.or.id/index.php/Ekonomi/article/view/1541

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. http://dx.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 and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation. *Pena Justisia: Media Komunikasi dan Kajian Hukum, 21*(2). http://dx.doi.org/10.31941/pj.v21i2.2680

Mangku, D. G. S., Yuliartini, 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). http://www.jsju.org/index.php/journal/article/view/813

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. http://dx.doi.org/10.1080/01900692

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. https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf

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. https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf

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. http://dx.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), 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. http://dx.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. http://dx.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 & Security Studies, 13*(4), 104-120. https://cejiss.org/addressing-indonesias-cyber-security-through-public-private-partnership-ppp

Setiyawan, A. (2019). National cybersecurity policy in the US and Indonesia. *UNTAG Law Review, 3*(1), 71-87. http://dx.doi.org/10.56444/ulrev.v3i1.1071

Sitompul, A., & Hasibuan, P. (2021). The Morality of Law Enforcement Agencies (Police, Prosecutor's Office, KPK) in Money Laundering With the Origin of the Corruption. *European Science Review,* (9-10), 55-63. https://doi.org/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: State estimation, attacks reconstruction and defense strategy. *Applied Mathematics and Computation, 413*, 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). https://www.researchgate.net/publication/324106226

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. *resmilitaris, 13*(1), 3110-3127. https://resmilitaris.net/menu-script/index.php/resmilitaris/article/view/1872

The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia

ORIGINALITY REPORT

12%	11%	3%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Michigan State University Student Paper	5%
2	www.ssoar.info Internet Source	4%
3	cybercrimejournal.com Internet Source	3%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		