Journal of Human Security | 2022 | Volume 18 | Issue 2 | Pages 62-69
DOI: 10.12924/johs2023.19010008
ISSN: 1835-3800

Journal of Human Security

Research Article

Cyber Criminology in Perspective of Human Security

Mohammad Fadil Imran

Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia
Email: mfadilimran@stik-ptik.ac.id
ORCID ID: https://orcid.org/0009-0007-3980-5518

Submitted: 15 July 2022 |In revised form: 7 October 2022 | Accepted: 21 December 2022 | Published: 30 December 2022

Abstract: This study examines Indonesia's evolving cyber landscape, marked by increasing internet usage and digital connectivity initiatives, which bring both opportunities and risks such as hacking, fraud, and infrastructure disruption. Through qualitative content analysis of over 100 academic works and legal documents spanning five years, the research evaluates the state of cyber criminality, assesses the efficacy of existing legal and policy frameworks, scrutinizes law enforcement capabilities and limitations, and suggests interlinked recommendations to enhance national cyber resilience. The findings reveal challenges including outdated legal frameworks, coordination issues in enforcement, limited public-private collaboration, and a scarcity of digital forensics expertise, hindering responses to privacy breaches, business disruptions, and financial fraud. The study proposes legal modernization, enhanced law enforcement training, robust identity frameworks, and public awareness initiatives to bolster cybersecurity governance, ensuring a balance between oversight, innovation, and rights protection.

Keywords: Cybersecurity, Cyber Criminology, Indonesia, Human Rights, Policy, Law Enforcement.

1. Introduction

Ensuring the security of Indonesia's expanding cyber ecosystem is imperative for its continued development and resilience. With over 200 million internet users and ranking as the fifth-largest market for social media globally, Indonesia's digital economy is projected to reach US$130 billion by 2025, fuelled by initiatives like "Making Indonesia 4.0." However, policymakers must urgently address the risks accompanying these transformative opportunities in cyberspace [1-3].

The advancements in 5G, artificial intelligence, encrypted platforms, augmented reality, biometric authentication, and quantum computing will shape behaviours, commerce, governance, infrastructure, and daily life for future generations [4, 5]. Beyond enhancing efficiency and economic prospects, technologies also introduce new threats, notably through cyberattacks targeting critical systems, privacy breaches, fraud, identity theft, industrial espionage, and the dissemination of child abuse material, among other concerns [6-8]. The abundance of sensitive online data heightens vulnerabilities, evident in data leaks and platform hacks impacting millions of Indonesian accounts in recent years. Safeguarding cyberspace integrity emerges as a strategic imperative given the surge in online activities such as financial transactions, telemedicine, academic credentialing, and democratic participation post-pandemic. However, this digital realm is now plagued by highly organized global syndicates and lone hackers, reaping billions annually from cybercrime with minimal risk compared to traditional crimes. Therefore, urgent changes to enable law enforcement and regulators to adapt to evolving technology are imperative [9-11].

The cohesion of various societal sectors in Indonesia, encompassing power grids, government records, and healthcare systems, fundamentally relies on the effectiveness of a robust cyberspace security apparatus. As digital connectivity extends across the archipelago, the allocation of resources towards cyber hygiene and risk awareness should be equitable with infrastructure development, falling within the purview of digital public goods. Instances such as the substantial exploitation of users through password-stealing malware in 2021 [12-14], and the hospital ransomware attack of 2020, which impeded pandemic response capabilities, underscore the tangible ramifications of cyber threats. In light of these events, defensive measures cannot be confined solely to technical units but necessitate the implementation of comprehensive organization-wide strategies that acknowledge the inevitability of technological oversights [15-17].

Indonesia's contemporary legal framework concerning cybersecurity is delineated across various Acts, Ministerial Regulations, and National Police procedures, among other regulatory instruments [18, 19]. Key legislative components encompass the 2008 Electronic Information and Transactions Law, supplemented by recent Government Regulation No. 71/2019, which delineates oversight authorities, cybersecurity governance duties, and guidelines for personal data usage [20-22]. Noteworthy are additional laws governing areas like money laundering, child protection, telecommunications security, domain administration, pornography regulation, and copyright. However, fragmented jurisdictions, ambiguous delineations of responsibilities, excessive specificity, and outdated technological parameters impede comprehensive enforcement against threats that possess the capability to transcend such limitations.

Cybersecurity attacks have evolved into industrial-scale operations, utilizing readily available online automated toolkits, with Indonesia's IP addresses ranking fifth among the world's most common origins for detected malware and ransomware threats

© 2023 by the authors; licensee Librello, Switzerland. This open access article was published under a Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

librello

[23]. Coupled with underdeveloped individual and organizational cyber hygiene practices, which annually lure millions through simplistic scams, often via common channels like SMS or mobile applications, the attack surface confronting law enforcement continues to expand. Despite possessing world-class technical specialists, high-performance computing infrastructure, and strategic planning capabilities essential for monitoring known threats, anticipation, investigation, and policy guidance, entities such as BSSN and regional forces require increased resourcing and collaboration with the private sector to mitigate risks from both overseas syndicates and exploitative domestic actors. This collaboration aims to safeguard citizens, infrastructure, institutions, and economic engines vital for livelihoods and communities across the nation. Responsibly nurturing local cyber talent is also critical, as coding becomes increasingly integrated into global school curriculums [24, 25].

Ransomware Attempts Against SMBs in Southeast Asia Prevented By Kaspersky				
Countries	2020		2019	
	Detections	Global Ranking	Detections	Global Ranking
Indonesia	439, 473	5	1, 158, 837	4
Malaysia	12, 191	56	67, 385	34
Philippines	22, 011	50	25, 946	45
Singapore	3, 191	78	2, 275	99
Thailand	122, 934	21	191, 281	22
Vietnam	204, 713	11	536, 586	7

Figure 1: Ransomware Attempts Reports in ASEAN Region (2019 and 2020).
Source: CyberSecurityAsean [23].

As nationwide efforts to connect people pay off, ethical technological progress can lead to positive changes in areas like access to education, microbusiness, efficiency gains, and environmental sustainability. These changes are possible as long as the right oversight systems are in place. But if people don't take care of their data, practice good cyber hygiene, get their jobs ready, and make sure the law works in a borderless, instantaneous cyberspace, unexpected problems or crimes could stop this potential from being realized. These problems could destroy the foundation of trust and resilience. The goal of this study is to look at the current state of cybercrime in Indonesia, including how well the country's policies and laws protect people from threats, as well as the government's and police's plans to fight cybercrime. It will also look at the problems and losses these plans cause and suggest important new directions that will help the country become more cyber-mature as risks rise.

2. Literature Review

2.1 Human Security Dimensions in Cyber Criminology

The human security dimension within cybercrime encompasses diverse facets of individual and societal well-being affected by cybercrimes. Cyber threats exert influence on human lives, freedom, and dignity [26]. One of the consequences pertains to the physical security of individuals, exemplified by instances such as bullying and online harassment, which precipitate psychological distress and overall harm, thereby affecting the mental health of individuals [27]. Cybercrimes lead to financial losses through fraud, affecting individuals' livelihoods. Online scams and financial fraud can cause hardship for individuals and may have broader economic implications if targeted at banks and financial institutions [28]. According to Hamid [29], the safety of people is also at risk because their private information and privacy can be viewed by people who aren't supposed to be there, which is called "breach of privacy." Cybercrime can also affect people's health. If medical data is stolen or fraud or false information about health care is spread, it can have an effect on a person's health. This is why the healthcare industry needs to be honest to protect data [30].

2.2 Cyber Criminology and Human Rights

The field of cyber criminology intersects with human rights, notably the right to privacy, wherein individuals possess the authority to control their information and communication. However, cybercrimes such as data theft, bullying, and data breaches have the potential to infringe upon these fundamental human rights [31]. Likewise, freedom of expression constitutes a fundamental entitlement of every individual. However, content blocking and censorship mechanisms impede the voices of individuals and hinder their ability to openly articulate their thoughts. As per Golose [32], individuals possess the entitlement to security, enabling them to live freely. However, cybercrimes, encompassing online harassment and bullying, can undermine human security, posing threats to both physical and mental well-being. Thus, the establishment of ethical and legal frameworks is imperative to safeguard human rights, privacy, and to hold those infringing upon privacy accountable.

2.3 Policy and Legal Frameworks for Human Security in Cyber Criminology

Policy and legal frameworks are pivotal in safeguarding human security, as evidenced by data protection and privacy laws such as the California Consumer Privacy Act and the European Union's General Data Protection Regulation. These regulations mandate data minimization, restrict the purposes for data usage, and empower users to manage and edit their personal data [32-34]. Likewise, cyber security legislation imposes requirements on organizations to fortify their systems against cyber threats. For instance, regulations like CISA and the Cyber Security Law of the People's Republic of China establish standards and prescribe their implementation within organizations. According to Chang [35], specific frameworks, such as the Universal Declaration of Human Rights and regional human rights treaties, safeguard individuals' rights to privacy and freedom of speech in the digital realm. Clear instructions and policy frameworks are crucial for the protection of human rights.

2.4 Cases of Cybercrime

Numerous instances of cybercrime significantly impact human well-being. One notable case is the Cambridge Analytica data scandal of 2018, which exposed the personal data of millions of Facebook users without their consent, utilized for political purposes, thereby raising substantial concerns regarding human rights and the unethical manipulation of personal data [36]. Similarly, the National Security Agency's surveillance program in 2013, involving the bulk collection of data from telecommunication networks, violated human rights and sparked debates regarding the balance between national security and individual privacy [37]. These real-world cybercrime incidents underscore the urgent imperative to safeguard individual rights and freedoms, fostering a secure environment for all.

2.5 Ways to Protect Human Rights Against Cybercrime

Abdullahi [38] assert that safeguarding human rights involves capacity building and training, which entails raising awareness among

individuals about cyber threats and educating users on preventing cybercrimes and safeguarding data. Moreover, employing encryption and multi-factor authentication enables users to protect their data, thereby upholding human rights. Implementation of data protection laws and educating individuals to limit data sharing are vital steps to mitigate risks and safeguard individual data [39]. Furthermore, aiding victims of cybercrime is paramount, encompassing counselling and legal assistance, alongside providing compensation for their losses. Collaboration among organizations and stakeholders is essential to safeguard human rights and ensure a safe and secure environment for individuals.

3. Method

This study employed a pragmatic, qualitative methodology, centred on an extensive examination of academic literature and legal documents concerning cybersecurity and cybercrime issues in Indonesia. Searches were conducted across scholarly databases such as Google Scholar, EBSCO, JSTOR, and Elsevier ScienceDirect, utilizing keywords including "Indonesia," "cybersecurity," "cybercrime," "human rights," "policy," and "law enforcement." Initial search results yielded over 100 articles, reports, and legal documents published within the preceding five years. These materials were systematically screened for relevance, focusing on works detailing cyber threats, impacts, and vulnerabilities among Indonesian citizens and systems, as well as the effectiveness of legal and policy countermeasures, and law enforcement capabilities and limitations. Only the most pertinent sources meeting these criteria underwent in-depth analysis using qualitative content analysis methods to extract information aligned with the study objectives.

4. Results

4.1 Status of Cyber Criminology in Indonesia

The incidence of cybercrime in Indonesia has exhibited rapid growth, facilitated by the expanding reach of the internet and smartphone usage. Indonesia's National Cyber and Crypto Agency (BSSN) reported a surge in cyberattacks, with over 290 million incidents recorded in 2019, representing a 25% increase compared to levels observed in 2018 [40]. These cyberattacks inflicted substantial economic losses on organizations within Indonesia [41, 42].

During the COVID-19 pandemic, there was a 40% surge in internet users, accompanied by 88 million cyberattacks in early 2020, notably phishing attempts, malware, and information gathering [40]. This surge of attacks jeopardizes individuals' finances and sensitive personal data, while also undermining businesses and government systems. Cybercrime encompasses a range of categories, including financial fraud and exploitation of women and children. According to the Indonesian police, common charges include online gambling, identity theft, insults/defamation, dissemination of immoral content, fraud, and intellectual property violations [43, 44]. Financial losses, reputational harm, and psychological suffering are prevalent consequences.

Children are particularly susceptible, as indicated by a study on sexual cybercrime cases which revealed that 20% of victims were under 18 years of age [45, 46]. Given children's increased online activity, they encounter elevated risks such as grooming, bullying, sexual solicitation, and self-generated problematic content [46, 47]. Urgent attention is needed to develop tailored prevention programs aimed at safeguarding children online.

4.2 Effectiveness of Legal Framework

Indonesia has implemented numerous legislative measures, notably the 2008 Electronic Information and Transactions (ITE) Law, addressing cyber activities. The ITE Law encompasses a range of offenses, including illegal access, data interference, misuse of electronic data, and online pornography [42, 48-50]. Various regulations cover consumer protection, money laundering, telecommunications, copyright, child protection, and domain name administration. Key regulations are outlined in Table 1.

Table 1: Key Laws and Regulations Related to Cybersecurity and Cybercrime in Indonesia.

Law/Regulation	Year	Summary
Law No. 36/1999 on Telecommunications	1999	Establishes offences related to misuse, illegal tapping, or distortion of telecommunications networks.
Law No. 28/2014 on Copyright	2014	Criminalizes unauthorized copying, distribution, or modification of protected works.
Law No. 8/2010 on Prevention and Eradication of Money Laundering	2010	Covers cybercrime proceeds and online transactions facilitating money laundering.
Law No. 44/2008 on Pornography	2008	Prohibits online pornography and sets penalties for creators/distributors of such content.
Law No. 20/2016 on Information and Electronic Transactions (ITE)	2016	A revised version of the ITE Law expanding cybercrime definitions and penalties.
Government Regulation No. 71/2019 on Implementation of Electronic Systems and Transactions	2019	Technical regulation mandating website authentication and personal data protection.
Law No. 17/2016 on State Intelligence	2016	Empowers intelligence agencies to conduct surveillance on electronic systems where national security threats are suspected.

Even though these laws are a step forward, experts point out that they don't cover all cybercrimes that happen across borders, they don't give police enough power, they're out of date, and it's not clear how power is divided between government departments [43, 51-54]. Most importantly, the speed at which new technologies allow for new types of hacking makes it hard for laws to keep up. Low reporting rates also hurt justice because many victims don't go to the police because they think the process is hard, expensive, and unlikely to get their losses back [54-56]. To properly take in cybercrime cases and perform investigations, law enforcement also needs more training, forensics tools, and public outreach.

Prosecutions depend a lot on expert evidence, but there aren't many certified forensic specialists in Indonesia [48, 57, 58]. Since the private sector has a lot of cybercrime expertise, tighter integration between the public and private sectors could make it easier to gather and analyses evidence. But there are problems with trust, openness, and possible conflicts of interest that get in the way. Implementing strong cybersecurity policies that rely on new regulatory frameworks is an ongoing process that is driven by regularly building up capabilities and creating adaptable methods that can adapt to fast changes in technology. After political debates about a new cybersecurity bill [59], progress is still slow. This shows how important it is to quickly reach a consensus while avoiding too broad measures that could stop innovation and make compliance too hard.

4.3 Government and Law Enforcement Strategies

Indonesia set up a National Cybersecurity Task Force in 2016 with the goal of coordinating policies, keeping an eye on threats, and guiding countermeasures across all departments [39, 60]. Even so, there is still a lot of governmental fragmentation when it comes to putting plans into action. BSSN

is at the centre of operations against cybercriminals, but so are units from the Defence Ministry, the National Police, the Justice Ministry, and regional cybercrime special teams. Indonesia's police school and regional training centres are working to improve the investigative skills of police officers in areas like digital forensics and cybercrime [47, 61]. Hacking methods, network protocols, data extraction, and malware analysis that criminals use are all covered in the course work. However, constant upgrades are necessary because technology changes so quickly these days.

In Jakarta, an innovative program trains former hacker to assist in tracking cybercriminals and bolster systemic resilience, provided they operate under supervision [62]. This initiative aims to reform individuals involved in information security violations, potentially enhancing cyber defence capabilities and offering alternative pathways for disadvantaged youth attracted to illegal cyber activities. Law enforcement agencies increasingly collaborate with universities, non-profit organizations, and technology firms to access expertise and collectively raise public awareness on cyber safety issues [42, 63]. However, private sector involvement remains limited, with critiques directed at legislative debates surrounding a proposed cybersecurity bill for insufficient industry input during its drafting phase [59]. Facilitating the sharing of threat data and incident reporting between companies and the government requires fostering an ecosystem of trust and mutual benefit.

While efforts are expanding across various fronts, systemic constraints such as under-resourcing, coordination challenges, a shortage of skilled personnel, public hesitancy in reporting incidents, and the need to monitor numerous entry points into Indonesia's networks hinder progress [48]. Sustained investments in both human capital and advanced cyber forensic tools are essential to enable enforcement agencies to pursue cybercriminals who often possess superior capabilities. With reported losses continuing to increase annually, intensifying progressive strategies and aligning legislation with technological realities appear crucial to safeguarding Indonesians in cyberspace.

5. Conclusion and Recommendations

Today's world is interconnected, bridging people across vast distances, and cyber criminology stands as a vital discipline examining the intersection of technology, crime, and human security [64, 65]. Cyber criminology investigates activities such as hacking, fraud, and cyberbullying. With increasing reliance on technology for communication and social interaction, it poses significant threats to individual, global security, and societal well-being [66]. Cybercrime significantly affects human security, encompassing physical safety and economic stability. The present study underscores that cyber threats should not solely be viewed as technical challenges but also through the lens of human security and well-being. It examines cyber criminology in light of the diverse impacts of cybercrime on human security, including physical, economic, financial, and mental dimensions [67, 68]. The study emphasizes the protection of human rights, such as privacy, freedom of expression, and security. Policy and legal frameworks offer guidelines and regulations to ensure the protection of human rights, implemented through capacity building, encryption, data protection laws, and victim support processes. Collaboration among stakeholders is essential to safeguard human privacy and foster an environment where individuals can utilize digital technology freely and without fear [69, 70].

The analysis of Indonesia's developing cybercrime scene within the context of the human security paradigm indicates increased vulnerabilities to online fraud, hacking, and data theft as a result of the country's quick internet adoption. Societies suffer grave consequences in terms of monetary losses, invasions of privacy, disruptions to commerce, and damage to infrastructure. The number of cases of identity theft, intellectual property violations, and internet distribution abuse rises year despite the country's superior cybersecurity, intelligence units, and several laws that criminalise these offences. This is due to inconsistent enforcement. The absence of public-private information interchange, the antiquated legal system, communication problems across ministries, and the shortage of skilled digital forensic investigators limit the kind of solutions that may be used to address international technical crimes. Since the initiatives promoting inclusive connection also offer opportunities and risks, it appears that resilient public awareness and advanced cyber defences are essential to maintaining national stability. The purpose of the following suggestions is to start a conversation about important future directions that the research's findings suggest.

5.1 Legal Frameworks & Enforcement

- Revise cybercrime law definitions and rules to consider the most recent developments in technology. This should include defining jurisdictional boundaries to facilitate regional collaboration.
- Seek to expedite the passage of a revamped cybersecurity bill that increases mandates and authorities while maintaining sufficient oversight and privacy protections.
- Enhance the instruction provided to law enforcement officials on dark web research, network monitoring, and digital forensic acquisition.
- Establish procedures and guidelines for the safe exchange of data breach reports and cyber threat intelligence with the least amount of liability exposure.
- To speed up prosecution, keep a national database of acknowledged cybersecurity specialists who are qualified to testify in court.

5.2 Human Security & Rights

- To protect kids, make programmes that teach people of all ages, especially parents and teachers, about how harassment and the risk of being sexually abused online work.
- Cyberbullying victims should have more access to therapy services and legal aid, as well as easy-to-use tools for getting help and recovering.
- To make e-government and financial services more secure as more things move online, you need to come up with reliable remote identification login methods that strike a balance between ease of access and privacy.
- Encourage more civilians to take part in policy talks about protecting human rights while increasing surveillance to stop threats.

6. Implications

The study and practice's results and suggestions have important theoretical and practical implications for the growth of cybersecurity in Indonesia, as well as policy implications.

Theoretically, studying the processes of cybercrime shows that cybervictimization, human security, and rights protection are all connected in ways that haven't been looked into much. The great majority of criminological literature that is about technology is about hacking, breaking into networks, and making tools for malware. More sociolegal views that focus on citizens' experiences and weaknesses can help the field of cybercriminal grow. Also, using a multidimensional human security risk scale to measure the effects of threats on areas like finances, health,

privacy, and damage to infrastructure shows that threats to society are linked in a lot more ways than just one crime or the economy. This is in line with current legal trends that put more emphasis on people's rights to grow, self-determination, and human dignity in cyberspace rather than seeing the internet as just a technical area for engineers and businesses.

In real life, the proposed legal and policy suggestions meant to speed up these actions include everything from programmes to teach parents and system administrators about cybersecurity to speeding up the passage of updated cybersecurity legal authority mandates that allow investigations to happen across borders. The goal is to help regulators and executives know what to focus on as they look for resources and implementation projects. This is done by giving them advice on how to make secure digital identity frameworks, expand law enforcement training, and encourage private sector intelligence sharing.

According to policymakers, looking into the gaps between Indonesia's laws and its ability to enforce them when it comes to new technological crimes means that the laws need to be updated with new attack vectors and updated on a regular basis. The region also needs to work together to stop transnational crime groups. The competition between the world's superpowers will make the issue of finding the right mix between oversight and protection of rights even more important. This is especially true when it comes to the touchy issues of surveillance and Internet freedom. These trends are likely to take over online in the long run.

7. Limitations and Future Research

The data for this analysis comes from a lot of important academic and legal papers, but there are some methodological limitations that should be considered. There are also other research areas that could be explored further. The assessment was based on qualitative reviews of literature and public documents. The results did not include direct field data from surveys or interviews with cybercrime victims, law enforcement, or policymakers to get their real-life experiences and points of view. Document analysis is useful for getting broad views, but hearing directly from stakeholders can help you get to the bottom of problems and realities on the ground. Also, the search method focused mostly on English-language books and legal documents, missing important discoveries that were only shown in Indonesian media. In turn, this has made the interpolative view less broad. Including sources written in the original language would make the analysis more valid and stop problems that happen when the analysis is focused only on English. When it comes to expanding study, three good directions stand out.

- *Comparative Assessments*

Comparing Indonesia's cybercrime and security to those in Southeast Asia and other emerging digital economies in the area would shed light on policy or advocacy efforts that could be used elsewhere. Transborder hacking groups change quickly, so knowing about the laws and signs of citizen exposure in other countries will help you guess how Indonesia will respond.

- *Surveys*

Systematic quantitative or qualitative surveys can be given to cybercrime victims, law enforcement units, and policymakers to get detailed information that can help figure out how people report cybercrime, how well investigations are going, where there are gaps in enforcement, and where there aren't enough resources. This information can then be used to come up with actionable steps to fix the problem based on real-life examples.

- *Ethnographies*

The ethnographic data from the field studies might show behaviours at a lower social level that affect people's weaknesses that aren't shown in the top-level review papers. Finding cases of social denigration or making a map of communication patterns in low-income migrant communities by watching how teens act online could show risks that were not seen before and need to be dealt with right away through education or tactics.

By addressing the problems that have been brought up through follow-up studies that use a variety of methods, such as cross-national comparisons, surveys, and ethnographic methods, there are important chances to improve practical solutions and academic knowledge about how criminology, human rights, and technological change interact in the global south in the 21st century.

References

[1] Wu P-J. Logistics business analytics for achieving environmental sustainability. Journal of Administrative and Business Studies. 2016;2(6):264-9. doi: https://doi.org/10.20474/jabs-2.6.1.

[2] Susilo D. Industry 4.0: Is Indonesia Ready? Management Analysis Journal. 2020;9(3):262-70. Available from: https://journal.unnes.ac.id/sju/index.php/maj/article/view/39695.

[3] Fernando Y, Wahyuni-TD IS, Gui A, Ikhsan RB, Mergeresa F, Ganesan Y. A mixed-method study on the barriers of industry 4.0 adoption in the Indonesian SMEs manufacturing supply chains. Journal of Science and Technology Policy Management. 2022. doi: https://doi.org/10.1108/JSTPM-10-2021-0155.

[4] Setiawan A, Muna A, Arumi E, Sukmasetya P. The Growth Electronic Commerce Technology and User Interface in Indonesia. Test Engineering and Management. 2020;83:16819-27. Available from: https://www.testmagzine.biz/index.php/testmagzine/article/view/10093.

[5] Hutajulu S, Dhewanto W, Prasetio EA. Two scenarios for 5G deployment in Indonesia. Technological Forecasting and Social Change. 2020;160:120221. doi: https://doi.org/10.1016/j.techfore.2020.120221.

[6] Aulianisa SS, Indirwan I. Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. Lex Scientia Law Review. 2020;4(1):31-45. Available from: https://journal.unnes.ac.id/sju/index.php/lslr/article/view/38197.

[7] Unlu A, Gurer C. Crime and Violence Studies in the Immigration Field. Journal of Ethnic and Cultural Studies. 2022;9(1):185-205. doi: https://doi.org/10.29333/ejecs/1021.

[8] Yusup DK. Cyber Security Sharing Platform: Indonesia Approach in Law Enforcement of Financial Transaction Crimes. Journal of Legal, Ethical and Regulatory Issues. 2022;25(2):1-22. Available from: https://www.abacademies.org/articles/Cyber-security-sharing-platform-Indonesias-1544-0044-25-2-104.pdf.

[9] Raza A. Laws Relating to Cyber Crimes: Theories and Legal Aspects. Available at SSRN 3066200. 2016. doi: https://dx.doi.org/10.2139/ssrn.3066200.

[10] Rawat M. Transnational Cybercrime: Issue of Jurisdiction. International Journal of Law Management and Humanities. 2021;4(2):253-66. doi: http://doi.one/10.1732/IJLMH.26049.

[11] Dayma D. Jurisdictional Challenges in Cyberspace-A Critical Legal Analysis of Legal Theories and Laws in India. In: Cyber Crime, Regulations and Security – Contemporary Issues and Challenges. The Law Brigade Publisher; 2022. p. 90-100. doi: https://doi.org/10.55662/book.2022CCRS.027.
[12] Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence. 2022;36(1):2037254. doi: https://doi.org/10.1080/08839514.2022.2037254.
[13] Ariani SR, Lumanto R. Study of Lokibot Infection Against Indonesian Network. OIC-CERT Journal of Cyber Security. 2022;4(1):85-96. Available from: https://www.oic-cert.org/en/journal/pdf/4/1/6.pdf.
[14] Chaudhary S, Kakkar R, Jadav NK, Nair A, Gupta R, Tanwar S, et al. A taxonomy on smart healthcare technologies: Security framework, case study, and future directions. Journal of Sensors. 2022;2022:1863838. doi: https://doi.org/10.1155/2022/1863838.
[15] Greenstein B. The Impact of Ransomware-as-a-Service on Critical Infrastructure [Doctoral Dissertation]. Utica University; 2022.
[16] He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of Medical Internet Research. 2021;23(4):e21747. doi: https://doi.org/10.2196/21747.
[17] Bernard R, Bowsher G, Sullivan R. Cyber security and the unexplored threat to global health: a call for global norms. Global Security: Health, Science and Policy. 2020;5(1):134-41. doi: https://doi.org/10.1080/23779497.2020.1865182.
[18] Ruhtiani M. Legal Protection of Traditional Architectural Design of Kampung Naga As Traditional Knowledge in Indonesia. UNTAG Law Review. 2021;5(1):54-64. doi: http://dx.doi.org/10.56444/ulrev.v5i1.2209.
[19] Stefano A, Endayani S, Sadono R. Combining the Traditional and Modern Architecture in Taman Samarendah Plan, Samarinda City, East Kalimantan Province, Indonesia. International Journal on Advanced Science Engineering Information Technology. 2021;11(2):705-11. doi: http://dx.doi.org/10.18517/ijaseit.11.2.8341.
[20] Waluyo TTP, Calista E, Ratu DP, Ramli TS, Ramli AM. The Indonesian Electronic Information and Transaction Within Indonesia's Broader Legal Regime: Urgency for Amendment? Jurnal Ham. 2021;12(3):533-52. doi: http://dx.doi.org/10.30641/ham.2021.12.533-552.
[21] Hartati S, Karyono H, Sabowo HK. Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia. International Journal of Educational Research and Social Sciences (IJERSC). 2022;3(1):425-32. doi: https://doi.org/10.51601/ijersc.v3i1.290.
[22] Dudley SE. The Office of Information and Regulatory Affairs and the durability of regulatory oversight in the United States. Regulation & Governance. 2022;16(1):243-60. doi: https://doi.org/10.1111/rego.12337.
[23] CyberSecurityAsean. Ransomware Targeting SEA SMBs Drops in 2020 vs 2019. 2021. Available from: https://cybersecurityasean.com/news-press-releases/ransomware-targeting-sea-smbs-drops-2020-vs-2019.
[24] Shahidullah K, Hossain R. Designing an Integrated Undergraduate Disaster STEM Curriculum. Journal of Ethnic and Cultural Studies. 2022;9(1):265-80. doi: https://doi.org/10.29333/ejecs/1042.
[25] Gonzales MMA, Palaca EJD, Iluis SLP, Tarusan MAE. Casting shadows of doubt: Perspectives of reputable journalists on fake news. Journal of Advances in Humanities and Social Sciences. 2018;4(6):267-78. doi: https://doi.org/10.20474/jahss-4.6.4.
[26] Salminen M, Hossain K. Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North. Polar Record. 2018;54(2):108-18. doi: https://doi.org/10.1017/S0032247418000268.
[27] Lee JK, Chang Y, Kwon HY, Kim B. Reconciliation of privacy with preventive cybersecurity: The bright internet approach. Information Systems Frontiers. 2020;22:45-57. doi: https://doi.org/10.1007/s10796-020-09984-5.
[28] Holt TJ. The Human Factor of Cybercrime. Routledge; 2019. doi: https://doi.org/10.4324/9780429460593.
[29] Hamid B, Jhanjhi N, Humayun M, Khan A, Alsayat A. Cyber security issues and challenges for smart cities: A survey. In: 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). IEEE; 2019. p. 1-7. doi: https://doi.org/10.1109/MACS48846.2019.9024768.
[30] Raina MacIntyre C, Engells TE, Scotch M, Heslop DJ, Gumel AB, Poste G, et al. Converging and emerging threats to health security. Environment Systems and Decisions. 2018;38:198-207. doi: https://doi.org/10.1007/s10669-017-9667-0.
[31] Brodowski D. Cybercrime, human rights and digital politics. In: Research Handbook on Human Rights and Digital Technology. Edward Elgar Publishing; 2019. p. 98-112. doi: https://doi.org/10.4337/9781785367724.00013.
[32] Golose PR. A comparative analysis of the factors predicting fears of terrorism and cyberterrorism in a developing nation context. Journal of Ethnic and Cultural Studies. 2022;9(4):106-19. doi: https://doi.org/10.29333/ejecs/1372.
[33] Chou C-H, Wu C-C, Lu K-C, Liu I-H, Chang T-H, Li C-F, Li J-S. Modbus packet analysis and attack mode for SCADA system. Journal of ICT, Design, Engineering and Technological Science. 2018;2(2):30-5. doi: https://doi.org/10.33150/JITDETS-2.2.1.
[34] Islam T, Becker I, Posner R, Ekblom P, McGuire M, Borrion H, Li S. A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems. In: International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications. Springer; 2019. p. 277-93. doi: https://doi.org/10.1007/978-981-15-1304-6_22.
[35] Chang V, Baudier P, Zhang H, Xu Q, Zhang J, Arami M. How Blockchain can impact financial services-The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change. 2020;158:120166. doi: https://doi.org/10.1016/j.techfore.2020.120166.
[36] Zhang F, Hines JW, Coble JB. A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. Nuclear Technology. 2020;206(7):939-50. doi: https://doi.org/10.1080/00295450.2019.1666599.

[37] Jawaid SA. Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. Preprintsorg. 2022. doi: https://doi.org/10.20944/preprints202211.0128.v1.
[38] Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, Abdulkadir SJ. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics. 2022;11(2):198. doi: https://doi.org/10.3390/electronics11020198.
[39] Siregar G, Sinaga S. The Law Globalization in Cybercrime Prevention. International Journal of Law Reconstruction. 2021;5(2):211-27. doi: http://dx.doi.org/10.26532/ijlr.v5i2.17514.
[40] Anjani NH. Cybersecurity protection in Indonesia. Center for Indonesian Policy Studies (CIPS), Jakarta; 2021. Available from: http://hdl.handle.net/10419/249442.
[41] Fatihah CYN. Indonesia's Approach on Cyberattack Attribution through its Foreign Policy. Global Legal Review. 2022;2(2):121-42. doi: http://dx.doi.org/10.19166/glr.v2i2.5140.
[42] Amin ME, Huda MK. Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. International Journal of Cyber Criminology. 2021;15(1):79-94. doi: https://doi.org/10.5281/zenodo.4766534.
[43] Jaelani NH. Tinjauan Viktimologis Terhadap Korban Tindak Pidana Cybercrime Illegal Content Di Wilayah Hukum POLRESTABES Bandung Dihubungkan Dengan Undang-Undang No 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik [Doctoral Dissertation]. UIN Sunan Gunung Djati Bandung; 2018. Available from: https://etheses.uinsgd.ac.id/id/eprint/9149.
[44] Prasetyo M. Legal Protection as a Form of State Responsibility for Victims of Cyber Crime in Indonesia. In: Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, ICETLAWBE 2020, 26 September 2020, Bandar Lampung, Indonesia. EAI; 2020. doi: http://dx.doi.org/10.4108/eai.26-9-2020.2302588.
[45] Arsawati INJ, Darma IMW, Antari PED. A criminological outlook of cyber crimes in sexual violence against children in Indonesian laws. International Journal of Criminology and Sociology. 2021;10:219-23. Available from: https://cdn.undiknas.ac.id/repository/REPO-16086009992229010.pdf.
[46] Bedi S. The Nuanced Forms of Sexual Violence in the Online Environment. In: Cyber Crime, Regulations and Security – Contemporary Issues and Challenges. The Law Brigade Publisher; 2022. p. 254-63. doi: https://doi.org/10.55662/book.2022CCRS.015.
[47] Saputra RW. A survey of cyber crime in Indonesia. In: 2016 International Conference on ICT For Smart Society (ICISS). IEEE; 2016. p. 1-5. doi: https://doi.org/10.1109/ICTSS.2016.7792846.
[48] Ardiansyah, Rafi M, Amri P. The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia. In: Moallem A, editor. HCI for Cybersecurity, Privacy and Trust. Cham: Springer International Publishing; 2022. p. 469-79. doi: https://doi.org/10.1007/978-3-031-05563-8_29.
[49] Djanggih H, Thalib H, Baharuddin H, Qamar N, Ahmar AS. The effectiveness of law enforcement on child protection for cybercrime victims in Indonesia. Journal of Physics: Conference Series. 2018;1028(1):012192. doi: https://doi.org/10.1088/1742-6596/1028/1/012192.
[50] Yuliartini NPR, Mangku DGS. Legal protection for women victims of trafficking in Indonesia in an international human rights perspective. International Journal of Criminology and Sociology. 2020;9(2):1397-404. doi: http://dx.doi.org/10.6000/1929-4409.2020.09.160.
[51] Offei MO. How does Victim Precipitation Theory explain Deviant Behaviours of Internet Romance Offenders? Gamer's Perspective of Victim Precipitation. International Journal of Technology and Management Research (IJTMR). 2021;6(2):59-72. Available from: http://journal.ktu.edu.gh/index.php/ijtmr/article/view/126.
[52] Erliyani R. Examining religious and justice system in Indonesia to prevent cyberbullying. International Journal of Cyber Criminology. 2022;15(2):112-23. Available from: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/23.
[53] Angkasa. Legal protection for cyber crime victims on victimological perspective. SHS Web of Conferences. 2018;54:08004. doi: https://doi.org/10.1051/shsconf/20185408004.
[54] Arwana YC. Victims of Cyber Crimes in Indonesia: A Criminology and Victimology Perspective. Semarang State University Undergraduate Law and Society Review. 2022;2(2):181-200. Available from: https://journal.unnes.ac.id/sju/index.php/lsr/article/view/53754.
[55] Mutiarin D, Pribadi U, Rahmawati DE. Overseeing Cyber-Neighborhoods: How Far the Indonesian National Police Effort in Handling Cybercrime? In: International Conference on Public Organization (ICONPO 2021). Atlantis Press; 2022. p. 549-55. doi: https://doi.org/10.2991/aebmr.k.220209.070.
[56] Khalid A, Charles S, Yasin Z, Tallat M. Antecedents of Rape Cases Exposure Over Social Media: A Comparative Study of Urban and Rural Areas of Lahore District. Journal of Management Practices, Humanities and Social Sciences. 2021;5(5):10-20. doi: https://doi.org/10.33152/jmphss-5.5.2.
[57] Marwan A, Jiow HJ, Monteiro K. Cybersecurity Regulation and Governance During the Pandemic Time in Indonesia and Singapore. International Journal of Global Community. 2022;5(1 (March)):13-32. Available from: https://www.riksawan.com/IJGC-RI/index.php/IJGC-RI/article/view/109.
[58] Amarullah AH, Runturambi AJS, Widiawan B. Analyzing cyber crimes during Covid-19 time in Indonesia. In: 2021 3rd International Conference on Computer Communication and the Internet (ICCCI). IEEE; 2021. p. 78-83. doi: https://doi.org/10.1109/ICCCI51764.2021.9486775.
[59] Aprilianti I, Dina SA. Co-regulating the Indonesian digital economy. Center for Indonesian Policy Studies (CIPS), Jakarta; 2021. Available from: http://hdl.handle.net/10419/249410.
[60] Hasbullah MA. Strategies and Best Practices Firms Should Adopt in Compliance with Business Competition Law: The Role of Cybercrime in Indonesian Perspective. International Journal of Cyber Criminology. 2022;16(2):87-103. Available from: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/97.
[61] Das S, Nayak T. Impact of cybercrime: Issues and challenges. International Journal of Engineering Sciences & Emerging Technologies. 2013;6(2):142-53. Available from: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

[62] Widiasari NKN, Thalib EF. The Impact of Information Technology Development on Cybercrime Rate in Indonesia. Journal of Digital Law and Policy. 2022;1(2):73-86. doi: https://doi.org/10.58982/jdlp.v1i2.165.
[63] Hasbullah MA. Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. International Journal of Cyber Criminology. 2022;16(2):119-30. Available from: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/112.
[64] Petersen RD. The Representation of the Women Presidents of the American Society of Criminology. American Journal of Qualitative Research (AJQR). 2020;4(3):66-83. doi: https://doi.org/10.29333/ajqr/8390.
[65] Dupont B, Whelan C. Enhancing relationships between criminology and cybersecurity. Journal of Criminology. 2021;54(1):76-92. doi: https://doi.org/10.1177/00048658211003925.
[66] Pachankis Y. Technical analysis on the cyber organizational criminology of dictatorial military conducts-experience from human trafficking and coercions by military cyber aggressions. International Journal of Security, Privacy and Trust Management. 2022;11(3):1-19. doi: https://doi.org/10.5121/ijsptm.2022.11301.
[67] A. D. Báez-Sánchez and N. Bobko, "Analysis of infected population threshold exceedance in an SIR epidemiological model," Letters in Biomathematics, 2021,doi: https://doi.org/10.30707/LiB8.1.1647878866.032781.
[68] M. Becker, R. Eigenfeld, and T. Kerpes, "Understanding the commercialization of intellectual property patents in Europe: Highlighting Implications and Regulations for the biotechnology sector," Journal of Commercial Biotechnology, vol. 28, no. 1, pp. 252-264, 2023, doi: https://doi.org/10.5912/jcb1902.
[69] E. C. Balreira, C. Hawthorne, G. Stadnyk, Z. Teymuroglu, M. Torres, and J. Wares, "Resources for supporting mathematics and data science instructors during covid-19," Letters in Biomathematics, vol. 8, no. 1, p. 49, 2021, doi: https://doi.org/10.30707/LiB8.1.1647878866.144285.
[70] J. Chen and H. Pang, "Analyzing Factors Influencing Student Achievement: A Financial and Agricultural Perspective Using SPSS Statistical Analysis Software," Journal of Commercial Biotechnology, vol. 28, no. 1, pp. 304-316, 2023, doi: https://doi.org/10.5912/jcb1118.