# Cyber Criminology: An analysis of the Indonesian and the United States Police Perception

***Mohammad Fadil Imran*[1]**
Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia

## Abstract
*This study compares police perceptions of cyber criminology in Indonesia and the United States, employing a "secondary qualitative research design." Findings reveal that Indonesia's cybercrime legislation requires amendments and lags behind technological advancements, despite existing regulations like the "Electronic Information and Transactions Law (UU ITE)." In contrast, the U.S. has a developed and effective cybersecurity system with dedicated agencies such as the "Department of Homeland Security (DHS)" and "Federal Bureau of Investigation (FBI)." The study contributes to the literature on police perception and offers insights for legal experts and law enforcement agencies to enhance laws and strategies for addressing cybercrime issues. The study acknowledges research limitations and provides future implications in the concluding section.*

**Keywords:** Cyber Criminology, Indonesia, United States, Police Perceptions.

## 1. Introduction
In the contemporary era of rapid technological progress, marked by the pervasive influence of digital advancements facilitating the global proliferation of cybercrime, the imperative to delve into the field of cyber-criminology has experienced a pronounced elevation in significance (Gilani et al., 2023; Golose, 2022a, 2023). In the context of Indonesia, a nation characterized by substantial technological advancement, law enforcement authorities encounter distinctive challenges stemming from the escalating prevalence of cybercrimes. The surge in internet connectivity and digital networks has resulted in a notable increase in cybercrimes, including identity theft and hacking, thereby posing additional complexities for law enforcement efforts in the country (Sumadinata, 2023). The Indonesian police face challenges in addressing cyber threats due to inadequate training, outdated legislation, and limited resources. Sociocultural factors, along with public ignorance and low confidence in police services, hinder effective intervention against online threats (Urane & Aminanto, 2023). In contrast, the United States law enforcement,

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

equipped with advanced technological infrastructure and ample resources, has taken the forefront in combating cybercrimes (Choi & Dulisse, 2023; Janet, Ajegbomogu, & John, 2020). The US police forces' perceptions of cybercrimes are influenced by their comprehensive knowledge of cyberspace, effective advanced training programs, and collaborations with foreign law enforcement agencies and industry experts (Alastal & Shaqfa, 2023). Stringent laws, such as the "Computer Fraud and Abuse Act," empower law enforcement to take strong action against cybercriminals. However, challenges persist, including the dynamic nature of cyberthreats and complex legal arrangements, necessitating ongoing technical innovation (Mijwil & Aljanabi, 2023).

Furthermore, Indonesia's cybercrime legislation is under development and frequently falls behind emerging technologies. Despite regulations like the "Electronic Information and Transactions Law (UU ITE)" framing cybercrime prosecution, certain offenses are inadequately addressed, and enforcement remains inconsistent. Societal factors, including widespread public distrust in the police and ignorance about cybersecurity, further impede effective measures against cybercrimes (Purnomo, 2023). Conversely, the United States has a more advanced and sophisticated cybersecurity system, driven by substantial investments in infrastructure, technology, and human resources. The government has established dedicated agencies, including the "Department of Homeland Security (DHS)" and the "Federal Bureau of Investigation (FBI)," to coordinate national cybersecurity efforts. Additionally, public-private partnerships, exemplified by programs like the "National Cybersecurity and Communications Integration Centre (NCCIC)," further enhance the nation's cybersecurity defences (Pala & Şana, 2020; Shestak & Tsyplakova, 2023). The existing literature on cyber criminology tends to favour Western perspectives, particularly those from the United States, overlooking diverse opinions from places like Indonesia. This results in an information gap concerning police perspectives and responses to cybercrime in different jurisdictions. By examining this comparative phenomenon, valuable insights can be gained into the effectiveness of tactics and resource allocation by US and Indonesian law enforcement. Understanding these differences is crucial for designing more nuanced and successful global approaches to combat cybercrime, promoting international cooperation in securing cyberspace. Therefore, the research aims to investigate how American and Indonesian law enforcement organizations perceive cybercrimes within the cybercriminal framework.

The research study comprises seven sections. Section 1 serves as the introduction. Section 2 conducts a literature review. Section 3 delineates the adopted research methodology. Section 4 elucidates the presented results. Section 5 offers conclusions and recommendations. Section 6 expounds upon the ramifications of the study. Lastly, Section 7 deliberates on the limitations of the current study and offers research directions for subsequent scholars.

## 2. Literature Review

### *2.1. Conceptualizing Cyber Criminology*

Cyber Criminology constitutes the scholarly investigation of criminal activities within a digital framework, encompassing phenomena such as hacking, identity theft, fraud, and cyberbullying (Jaishankar, 2018). This field examines the causation and repercussions of these activities on individuals, organizations, and businesses.

*2.2. Police Significance and Perception*

Police perception refers to how law enforcement officers, based on their professional roles, comprehend cybercrime, shaping their attitudes, beliefs, and influencing societal impact (Hadlington et al., 2021). The police's perception of cybercrime significantly affects resource allocation, law enforcement, and investigative strategies aimed at preventing such crimes. As asserted by Dupont and Whelan (2021), the police play a pivotal role in addressing digital offenses, involving crime prevention through public awareness campaigns and educational initiatives to promote secure online practices. Additionally, police departments contribute to the investigation of criminal activities, employing forensic techniques to gather evidentiary support (Ashaari et al., 2023; Cockcroft et al., 2021). Police collaborate with government, private institutions, and educational entities to share expertise, fostering intelligence sharing and best practices. Additionally, they offer training and capacity building for officers to enhance their skills and knowledge (Harkin & Whelan, 2022). Overall, the police play a crucial role in preserving cybersecurity and safeguarding the populace from potential threats.

*2.3. Cyber Criminology Laws in Asian & Eurasian Countries*

Cybercrime legislation exhibits variability across nations, although common legislative measures are implemented to mitigate cyber risks. In Japan, the Basic Act on Cybersecurity serves as a legal framework addressing cybercrime, specifically targeting unauthorized access to systems (Simonov, Klenkina, & Shikhanova, 2020). Likewise, Singapore has witnessed an increase in cybercrime and enacted the Computer Misuse Act to oversee computer-related offenses. China, as a leading global economy, has not been exempt from cybercrime and has instituted regulations such as the Cybersecurity Law, governing network operations and security. Simultaneously, the Criminal Law of the People's Republic of China provides counselling for victims of cybercrime, including identity theft, cyberbullying, and hacking, holding perpetrators accountable (Yu, 2018). In recent years, Indonesia has witnessed a surge in cybercrime, encompassing activities such as fraud, identity theft, cyberbullying, and hacking, facilitated by the widespread adoption of technology (Arwana, 2022). To counteract these offenses, Indonesia has implemented various laws, including the Electronic Information and Transactions Law, which establish regulations and frameworks for addressing cybercrime (Marliyanti, 2023). However, law enforcement agencies in Indonesia face challenges due to limited resources and expertise in addressing cyber threats, necessitating attention and facilitation of police capabilities in forensic analysis, investigation, and evidence collection (Jhon, 2018). A crucial aspect of Indonesia's cybercrime prevention strategy involves enhancing public awareness through digital literacy initiatives, employing awareness campaigns to educate individuals about potential frauds. Sustained efforts and continual investment in cyber security capabilities are imperative for effectively addressing the evolving challenges in Indonesia's cyber criminology landscape (Jhon, 2018).

As per Kethineni (2020), India has enacted the Information Technology Act of 2000, which includes provisions for legal recognition, data protection, privacy, and cyber offenses to safeguard individual security and privacy. In the United States, a diverse array of cyber threats, including data breaches, ransomware, and online fraud, is addressed

through legislation such as the Computer Fraud and Abuse Act, Cyber Security Information Sharing Act, and Electronic Communication Privacy Act, establishing a legal framework to prevent cybercrime and secure digital data (Jaishankar, 2018). Within the United States, law enforcement entities such as the Federal Bureau of Investigation, the Secret Service, and various police departments exhibit capabilities in digital forensics and investigation. In Turkey, the Internet Law serves to monitor internet usage and establish regulations pertaining to online defamation and cyberbullying (Ar & Caglar, 2021). Similarly, Russia has enacted specific laws, such as the Federal Law on Information, Information Practices, and Technologies, along with provisions in the Criminal Code of the Russian Federation addressing fraud and unauthorized data access (Dremliuga, Dremliuga, & Kuznetsov, 2020).

### *2.4. Comparative Analysis of Indonesian and US Police Perception*

In Indonesia, police perception of cybercrime is primarily shaped by the crime's severity, impact on individuals and businesses, and resource constraints (Bawono, 2019). In the United States, the scale of the crime, particularly high-profile cyber incidents, informs police awareness of potential impacts (Cross et al., 2021; Manu & Ntsaba, 2016). Indonesian police prioritize community engagement and awareness to respond to cyber threats, while U.S. police focus on investigation strategies, capacity-building through training, and resource allocation. Cultural factors, trust in law agencies, and societal attitudes towards cybercrime influence Indonesian police perception, whereas in the U.S., the role of government and individual rights shapes police perspectives on cybercrime (Bawono, 2019; Cross et al., 2021).

### *2.5. Cases Regarding Police Involvement in Cybercrime*

For reasons of confidentiality, the details of many police cases remain inaccessible to the public; however, researchers have discussed notable cybercrimes, among them the Target Data Breach of 2013. In this incident, hackers illicitly obtained credit and debit card information from thousands of customers during the holiday season, constituting one of the most extensive security breaches. The law enforcement response to this event involved agencies such as the FBI, underscoring the pivotal role of law enforcement entities in addressing significant cyber threats (Khalid et al., 2021; Plachkinova & Maurer, 2018). Another notable cybercrime event is the WannaCry Ransomware Attack in 2017, wherein criminals globally targeted computers running Microsoft Windows, encrypting data and demanding ransom payments in bitcoin. Collaborative efforts between law enforcement agencies, including Europol and the United States Department of Justice, were employed to investigate the incident (Hsiao & Kao, 2018). Additionally, the Equifax Data Breach of 2017, as outlined by Kenny (2018), exposed sensitive information of more than 140 million consumers. The Federal Trade Commission and the U.S. Securities investigated the case, attributing responsibility for data protection failure to the organization itself.

## 3. Research Methodology

To investigate cyber criminology perspectives of U.S. and Indonesian law enforcement, a normative qualitative method was employed for data collection. This approach prioritizes normative frameworks guiding law enforcement perceptions

and responses to cybercrime in both countries. Data was gathered from primary sources such as laws, rules, legislation, and case laws pertaining to cybercrime in the U.S. and Indonesia. These primary sources offered crucial insights into legal aspects and police procedures. Additionally, secondary sources, including journal articles, books, literature reviews, relevant textbook chapters, and other academic materials, were utilized to complement the study alongside primary sources. Academic inquiries into cybercrime issues and law enforcement perspectives were facilitated through diverse online platforms like West Law, JSTOR, Lexis, Wiley Internet, and other reputable sites. Employing both primary and secondary sources, a comprehensive content analysis was undertaken, encompassing diverse opinions and factual information to substantiate interpretations. Rigor and validity of the study findings were enhanced through methodological triangulation and the utilization of varied sources. This method facilitated the examination of socio-legal, cultural, and institutional factors influencing police perceptions in Indonesia and the U.S., thereby elucidating the intricate nature of cybercrime and law enforcement responses by incorporating numerous legal texts, documents, references from academic literature, and empirical studies.

## 4. Results and Discussion

### *4.1 The United States and Indonesia Working Together to Combat Cyberterrorism in Indonesia*

The United States and Indonesian governments are grounded in democratic principles. Nurturing and fortifying connections to address disparities and foster a sense of maturity and responsibility is achievable through democratic partnerships. The enhancement of relations between the two nations necessitates collaborative efforts from the executive branches of Indonesia and the United States. Furthermore, heads of government departments engage in regular meetings to cultivate diplomatic ties. U.S.-Indonesia relations are predicated on shared interests, encompassing security cooperation within their bilateral relationship and collaborative efforts to establish a new security architecture for the Asia-Pacific region—an arena where substantial cooperation between the United States and Indonesia has been fostered (Gonzales et al., 2018; Putra, 2022).

The integration of the National Action Plan for Countering Extremism in Indonesia with the governmental strategy aimed at addressing terrorism through nuanced approaches is reflected in the President Regulation on Counterterrorism. This regulatory framework incorporates various measures designed to mitigate terrorist attacks and the propagation of violent extremism. The involvement of multiple ministries and relevant entities is envisioned for the coordinated execution of these measures. The overarching objective is the reduction of terrorist incidents and the curbing of extremist activities. This regulatory instrument is intended to complement existing anti-terrorism legislation and policies, with particular emphasis on strategies to combat extremism. Effective counterterrorism and the prevention of violent extremism necessitate the concerted coordination of efforts across diverse governmental departments and agencies. Facilitating the engagement and cooperation of both civil society and governmental bodies is imperative in the collective endeavour to combat violent extremism (Anwary, 2022).

The article also discusses the utilization of human resources to proactively monitor, identify, and prevent acts of extremism. Additionally, it addresses strategies for supporting individuals who have fallen victim to terrorist crimes (Ramadhan, 2023).

*4.2 BSSN's Cyber Cooperation in Countering Cyberterrorism*

The National Cyber and Code Agency (BSSN), pivotal in US-Indonesia cyber collaboration, has implemented initiatives aligned with the four-year goals outlined in the 2018 Letter of Intent (LoI). Assessing accomplishments and progress is vital to understanding the significance of this cooperation in advancing cybersecurity in Indonesia. Bilaterally, Indonesia engages in cybersecurity cooperation with ten countries, including the US, UK, Russia, China, Australia, Saudi Arabia, Poland, Turkey, Qatar, and the Czech Republic. The US-Indonesia LoI aims to establish a foundation for cyber cooperation and capacity building, encompassing discussions on cybercrime capacity, multi-stakeholder partnerships, cyber awareness promotion, incident management capabilities, cybercrime strategy development, and regional cooperation (Golose, 2022b; Luu et al., 2019).

Through communication channels established via the US Embassy in Jakarta, the BSSN has facilitated coordination and collaboration in the cyber domain, particularly with representatives from the FBI, to execute agreed-upon areas of cooperation within the Indonesia-US cyber cooperation framework. Efforts are underway to enhance human resource capabilities through training and webinars, alongside disseminating information regarding cyberattack risks. The number of BSSN cyber personnel undergoing capacity building within the RI-US cyber cooperation serves as one performance indicator from the BSSN perspective. Additionally, anticipatory measures or actions aimed at mitigating the impact of cyber threats resulting from bilateral information sharing cooperation serve as another indicator. Administrative hurdles, such as discrepancies in program execution timelines between the US Embassy and BSSN, frequently challenge the implementation of cooperation agreements by BSSN (Chou et al., 2018; Putra, 2022; Urane & Aminanto, 2023). Moreover, BSSN anticipates encountering challenges in coordinating with other cyber-related authorities, given the interdisciplinary nature of cybersecurity that traverses various sectors. Thus far, in the execution of the designated areas of collaboration within the RI-US cyber cooperation framework, BSSN has initiated communication channels via the US Embassy in Jakarta. The embassy has facilitated cyber domain coordination and collaboration, exemplified by engagements with FBI officials.

*4.2.1 Capacity Building*

Collaboration between the Défense Cyber Operations Centre and training programs is crucial for enhancing cybersecurity capabilities. Human resources training is vital to raise awareness and take preventive measures against cybercrime. The TNI has partnered with IT leaders, including the North Sumatran Del Institute of Technology (IT Del), to train personnel in cybersecurity. Three programs were planned for the 2014-2017 partnership, as described by Rizal and Yani (2016). BSSN will host the Virtual Homeland Security Investigation (HSI) Online Investigation from March 14-16, 2022, in collaboration with the U.S. Embassy, involving members from the Cybersecurity Strategy and Ciphers Directorate. This initiative is expected to yield significant outcomes:

- Enhancing skills in handling digital evidence should be a key objective in combating international crime and human trafficking.
- Secondly, engaging in discussions covering areas such as dark site investigations, digital forensics, and international crimes.
- Disseminating knowledge and setting standards for endeavours related to cyber networks.

*4.2.2 Information Sharing*

As per Sandy et al. (2023), cyber power conventionally denotes the capacity to operate within cyberspace, emphasizing the importance of information exchange. Technology facilitates entry into the cyber realm, making its utilization inherent. Given the dynamic nature of technology, entities like governments, societies, and non-state actors can leverage emerging technologies for substantial benefits.

Acquiring information via cyberspace can enhance a nation's cyber power quotient, enabling the wield of soft power in policymaking and international affairs, thereby benefiting the nation. The concept of power is recognized for its influence on domestic decisions and the establishment of hegemony. An effective information-sharing initiative can aid countries in combating cyber threats, including cyber terrorism.

*4.2.3 Handling Cyberterrorism*

The Indonesian government is obligated to respond promptly in accordance with prevailing laws and regulations. Individuals or groups propagating fake news, intolerance, hostility, intolerance towards differences, and extremism are subject to Law No. 19 of 2016, which amends the Information and Electronic Transactions Law 11 of 2008 (Yumitro et al., 2023).

Putra (2022) posited that cyberterrorism is the convergence of terrorism and cyberspace, involving threats or attacks against computers, networks, and stored information with the intent to intimidate governments and societies for political or social motives. For an act to be classified as cyberterrorism, it must pose a potential threat to a nation and be conducted online. Effective coordination between BSSN and BNPT is imperative in combating cyberterrorism.

## 5. Conclusion and Recommendations

The comparative analysis of police perceptions regarding cybercrime in the United States and Indonesia highlights significant disparities in approach, capabilities, and resources. The study underscores Indonesia's unique challenges in combating cybercrimes, characterized by outdated legislative frameworks, resource constraints, and public unawareness of cybersecurity issues. In contrast, the United States exhibits a more advanced cybersecurity infrastructure, with ample resources and sophisticated training programs for law enforcement agencies. While Indonesia's cybercrime legislation is still evolving and struggling to keep pace with technological advancements, the United States has comprehensive laws such as the Computer Fraud and Abuse Act to empower law enforcement agencies. Indonesia prioritizes public awareness and engagement to effectively counter cyber threats, while the US

emphasizes investigative strategies and capacity-building through training programs. The collaboration between Indonesia and the United States in addressing cyberterrorism underscores the necessity of international cooperation in addressing cyber threats. Initiatives such as Indonesia's National Action Plan to counter extremism and bilateral cyber cooperation efforts exemplify global endeavours to enhance cybersecurity.

Based on the discussion and in-depth analysis, following recommendations can be provided:

1. Indonesia must prioritize the establishment and enhancement of cybercrime legislation to effectively address emerging threats. This entails prosecuting cyber-related offenses and ensuring consistent enforcement.
2. Indonesia's law enforcement agencies should prioritize investment in cybersecurity infrastructure, training programs, and capacity-building initiatives to enhance their capabilities in combating cybercrimes.
3. Efforts should focus on educating the public about cybersecurity risks and best practices to mitigate them. Awareness campaigns can empower individuals and ensure online protection.
4. Indonesia should prioritize enhancing collaboration with nations like the United States to address cyberterrorism, ensuring the adoption of best practices in cybersecurity. Additionally, fostering collaboration between BSSN and BNPT can effectively mitigate cyber threats.

## 6. Research Implications

The current study holds various theoretical and practical implications, which are elaborated upon as follows:

The current study adds to the body of research by focusing on how sociocultural factors significantly affect how law enforcement agencies feel about hacking. The way people in different countries believe police and how they feel about cybersecurity are also cultural factors that have an impact on how police see things and how they respond in different countries. This study also shows how important laws are in shaping how people think about the police and how they fight cybercrime. On the other hand, the fact that Indonesian and US hacking laws are different is also a big part of figuring out how well law enforcement is working. Before this study, there wasn't a lot of research that looked at cybercriminal from the point of view of both Indonesian and US police. Because of this, this study adds to the growing body of literature on the subject of study.

This work is also very important in the real world. This study has shown how important it is to change the laws right away in places like Indonesia where hacking laws aren't very good yet. Policymakers can also learn from this study by setting the goal of updating legal frameworks as a top priority. This will give law enforcement the tools they need to effectively deal with new online threats. This study also showed that more money needs to be put into building up the infrastructure for cybersecurity and teaching and building up the skills of the agencies that are supposed to enforce the law. It also has real-world effects on how important it is for countries to work together.

## 7. Research Limitations and Future Indications

There are a number of limitations that must be addressed, even though the comparative study of police perceptions of cybercrime in Indonesia and the United States provides insightful information. First off, the study's reliance on previously published work and secondary data sources has constrained its scope and ignored more recent developments relevant to this topic. Furthermore, the viewpoints of other pertinent stakeholders have been overlooked in favour of a primary focus on police perception in this study. These could include governmental officials, cybersecurity specialists, and members of the general public. There is also a constraint on the availability and dependability of the data in this study. It particularly has to do with the private data involved in the cybercrime investigation. Future research endeavours ought to endeavour to tackle these constraints by including primary data collection techniques, engaging a diverse range of stakeholders, and remaining abreast of evolving trends and advancements in the field of cyber criminology. Future researchers can also conduct interviews with legal professionals in the United States and Indonesia to compare their perspectives and opinions and get better findings. Primary qualitative data might be useful in deriving significant conclusions from interview findings. Due to the cross-sectional structure of the study, data collection and analysis are also part of the current investigation at a certain point in time. In order to get more useful data, future researchers can apply a longitudinal strategy and evaluate related topics.

## References

Alastal, A. I., & Shaqfa, A. H. (2023). Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool. *Journal of Data Analysis and Information Processing, 11*(2), 121-143. https://doi.org/10.4236/jdaip.2023.112008

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology, 16*(2), 216-227. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/135

Ar, G., & Caglar, I. (2021). Evaluation under Turkish Criminal Law of Crimes Committed in the Cyber World. *GSI Articletter, 24*, 138. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gsiartc24&section=13

Arwana, Y. C. (2022). Victims of Cyber Crimes in Indonesia: A Criminology and Victimology Perspective. *Semarang State University Undergraduate Law and Society Review, 2*(2), 181-200. https://doi.org/10.15294/lsr.v2i2.53754

Ashaari, M. F., Norhisham, N. A. S., Subramaniam, P., Manap, J., & Abd, H. (2023). Adapting Social Supports through Communication Technologies as a Lifelong Learning for Older Adults. *Pakistan Journal of Life and Social Sciences, 21*(1), 205-220. https://doi.org/10.57239/PJLSS-2023-21.1.0017

Bawono, B. T. (2019). Reformation of Law Enforcement of Cyber Crime in Indonesia. *Jurnal Pembaharuan Hukum, 6*(3), 332-349. http://dx.doi.org/10.26532/jph.v6i3.9633

Choi, J., & Dulisse, B. (2023). Techno-crime prevention: the role of the private sector and its partnerships with the public sector. In *Handbook on Crime and Technology* (pp. 359-374). Edward Elgar Publishing. https://doi.org/10.4337/9781800886643.00030

Chou, C.-H., Wu, C.-C., Lu, K.-C., Liu, I.-H., Chang, T.-H., Li, C.-F., & Li, J.-S. (2018). Modbus packet analysis and attack mode for SCADA system. *Journal of ICT, Design, Engineering and Technological Science, 2*(2), 30-35. https://doi.org/10.33150/JITDETS-2.2.1

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C., & Trevorrow, P. (2021). Police cybercrime training: perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice, 15*(1), 15-33. https://doi.org/10.1093/police/pay078

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends and Issues in Crime and Criminal Justice [electronic resource],* (635), 1-20. https://doi.org/10.52922/ti78207

Dremliuga, R., Dremliuga, O., & Kuznetsov, P. (2020). Combating the Threats of Cybercrimes in Russia: Evolution of the Cybercrime Laws and Social Concern. *Communist and Post-Communist Studies, 53*(3), 123-136. https://doi.org/10.1525/cpcs.2020.53.3.123

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology, 54*(1), 76-92. https://doi.org/10.1177/00048658211003925

Gilani, S. R. S., Mujtaba, B. G., Zahoor, S., & AlMatrooshi, A. M. (2023). Exploring cybercrime history through a typology of computer mediated offences: Applying Islamic principles to promote good and prevent harm. *Computing and Artificial Intelligence, 1*(1), 321. https://ojs.acad-pub.com/index.php/CAI/article/view/321

Golose, P. R. (2022a). A comparative analysis of the factors predicting fears of terrorism and cyberterrorism in a developing nation context. *Journal of Ethnic and Cultural Studies, 9*(4), 106-119. https://doi.org/10.29333/ejecs/1372

Golose, P. R. (2022b). Cyber Terrorism-A Perspective of Policy Analysis. *International Journal of Cyber Criminology, 16*(2), 149-161. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/118

Golose, P. R. (2023). Terrorism as Socio-Economic and Cultural Barriers to Indonesian Firms' Financial Performance. *Journal of Ethnic and Cultural Studies, 10*(2), 22-40. https://doi.org/10.29333/ejecs/1536

Gonzales, M. M. A., Palaca, E. J. D., Iluis, S. L. P., & Tarusan, M. A. E. (2018). Casting shadows of doubt: Perspectives of reputable journalists on fake news. *Journal of Advances in Humanities and Social Sciences, 4*(6), 267-278. https://doi.org/10.20474/jahss-4.6.4

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2021). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice, 15*(1), 34-43. https://doi.org/10.1093/police/pay090

Harkin, D., & Whelan, C. (2022). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management, 24*(1), 66-76. https://doi.org/10.1177/14613557211036565

Hsiao, S.-C., & Kao, D.-Y. (2018). The static analysis of WannaCry ransomware. In *2018 20th international conference on advanced communication technology (ICACT)* (pp. 153-158). IEEE. https://doi.org/10.23919/ICACT.2018.8323680

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology, 12*(1), 1-8. https://www.cybercrimejournal.com/pdf/JaiEditorialVol12Issue1IJCC2018.pdf

Janet, A. S., Ajegbomogu, J., & John, M. D. (2020). Night-guards: Exploring gain and losses. *Journal of Advances in Humanities and Social Sciences, 6*(1), 10-18. https://doi.org/10.20474/jahss-6.1.2

Jhon, R. M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. *IJCLS (Indonesian Journal of Criminal Law Studies), 3*(1), 25-34. https://doi.org/10.15294/ijcls.v3i1.16945

Kenny, C. (2018). The Equifax Data Breach and the Resulting Legal Recourse. *Brooklyn Journal of Corporate, Financial & Commercial Law, 13*(1), 10. https://brooklynworks.brooklaw.edu/bjcfcl/vol13/iss1/10

Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 305-326). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_7

Khalid, A., Charles, S., Yasin, Z., & Tallat, M. (2021). 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, 5*(5), 10-20. https://doi.org/10.33152/jmphss-5.5.2

Luu, P. V., Weed, J., Rodriguez, S., & Akhtar, S. (2019). An AI-based web surveillance system using raspberry Pi. *Journal of Advances in Technology and Engineering Research, 5*(6), 231-242. https://doi.org/10.20474/jater-5.6.2

Manu, E., & Ntsaba, M. J. (2016). Perceptions of marijuana use: Chronicles of marijuana smokers from two marijuana-Growing communities in South Africa. *Journal of Advances in Health and Medical Sciences, 2*(3), 82-91. https://doi.org/10.20474/jahms-2.3.1

Marliyanti, M. (2023). Optimization of Cyber Law as A Legal Basis for Handling Cyber Crime in Indonesia. *JLASA (Journal of Law and State Administration), 1*(1), 8-12. https://journal.yhmm.or.id/index.php/JLASA/article/view/3

Mijwil, M., & Aljanabi, M. (2023). Towards artificial intelligence-based cybersecurity: the practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal For Computer Science and Mathematics, 4*(1), 65-70. https://doi.org/10.52866/ijcsm.2023.01.01.0019

Pala, Z., & Şana, M. (2020). Attackdet: Combining web data parsing and real-time analysis with machine learning. *Journal of Advances in Technology and Engineering Research, 6*(1), 37-45. https://doi.org/10.20474/jater-6.1.4

Plachkinova, M., & Maurer, C. (2018). Security Breach at Target. *Journal of Information Systems Education, 29*(1), 11-20. https://aisel.aisnet.org/jise/vol29/iss1/7

Purnomo, V. D. (2023). Transaction Fraud Buy and Sell Online Through Restitution as Criminal Addition in the Electronic Information and Transaction Law. *Asian Journal of Community Services, 2*(3), 265-286. https://doi.org/10.55927/ajcs.v2i3.3548

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

Ramadhan, I. (2023). ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities. *Journal of Social and Political Sciences, 6*(4), 1-10. http://dx.doi.org/10.31014/aior.1991.06.04.440

Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies, 4*(1), 61-78. https://dx.doi.org/10.21512/jas.v4i1.967

Sandy, M. R. A., Ras, A. R., Yusnaldi, Y., Widodo, P., & Suwarno, P. (2023). The Impact Of Cyber Espionage Issue On Maritime Security Cooperation Between Indonesian National Police And Australian Federal Police. *International Journal Of Humanities Education and Social Sciences, 3*(2), 866-874. https://doi.org/10.55227/ijhess.v3i2.708

Shestak, V., & Tsyplakova, A. (2023). Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA. *Brics Law Journal, 10*(4), 35-52. https://doi.org/10.21684/2412-2343-2023-10-4-35-52

Simonov, N., Klenkina, O., & Shikhanova, E. (2020). Leading Issues in Cybercrime: A Comparison of Russia and Japan. In *6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019)* (pp. 504-510). Atlantis Press. https://doi.org/10.2991/assehr.k.200526.073

Sumadinata, W. S. (2023). Cybercrime and Global Security Threats: a Challenge in International Law. *Russian Law Journal, 11*(3), 438-444. https://doi.org/10.52783/rlj.v11i3.1112

Urane, I., & Aminanto, M. E. (2023). The Role of Hybrid and Community-oriented Policing in the Future Management of Cybercrime in Indonesia: Lesson Through Comparison. *The Seybold Report, 18*(1), 1-22. https://doi.org/10.17605/OSF.IO/HYP5S

Yu, Z. (2018). Internet Criminal Law in China: Cybercrime Transformations, Legislative Examples, and Theoretical Contributions. *Zeitschrift für die gesamte Strafrechtswissenschaft, 130*(2), 555-581. https://doi.org/10.1515/zstw-2018-0022

Yumitro, G., Febriani, R., Roziqin, A., & Oktaviani, S. (2023). New model of terrorism threat in Indonesia: East Java case study. *Journal of Liberty and International Affairs, 9*(3), 234-247. https://doi.org/10.47305/JLIA2393216y