Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

Islamic Legal Perspective on Cybercrime: An Ethical and Legal Analysis of Contemporary Challenges in Digital Responsibility

Muhammad Ruslan Afandi
Universitas Harkat Negeri, Tegal, Indonesia
e-mail: mruslanafandi@harkatnegeri.ac.id

Article Information
Received : December 07, 2025 Revised : December 24, 2025 Accepted : December 31, 2025

ABSTRACT

Cybercrime is increasingly prevalent in Indonesia, impacting individuals, society, and national security. **This paper explores** various forms of cybercrime through the perspective of Islamic law, highlighting violations of justice, honesty, and the prohibition of wrongdoing. Adopting a **descriptive qualitative approach**, the study draws on secondary data from BSSN, Kominfo, UNICEF, Mafindo, and scholarly literature published between 2020 and 2025. **Data collection** involved thematic analysis to identify patterns, trends, and socio-legal impacts. **The findings** reveal a consistent rise in cases and damages, predominantly stemming from internet fraud and data breaches. Islamic law regards cybercrime as a serious breach of justice, integrity, and moral conduct, emphasizing the critical role of digital ethics and personal accountability in the online environment. Uniquely, **this study bridges a gap** in existing literature by offering an integrative analysis of Islamic legal principles and contemporary cybercrime challenges an area that remains underexplored. The research underscores the importance of synthesizing regulatory frameworks, educational initiatives, and ethical standards to bolster cybersecurity. Additionally, it advocates for continuous policy development, the incorporation of religious ethics in digital education, and enhanced international cooperation, **thus contributing** both theoretical and practical insights to the discourse on cybercrime prevention within an Islamic legal context.

Keywords: cybercrime, islamic law, and digital responsibility

ABSTRAK

Kejahatan siber semakin marak di Indonesia, berdampak pada individu, masyarakat, dan keamanan nasional. ***Artikel ini mengeksplorasi*** *berbagai bentuk kejahatan siber melalui perspektif hukum Islam, menyoroti pelanggaran terhadap keadilan, kejujuran, dan larangan berbuat salah. Menggunakan pendekatan* ***kualitatif deskriptif****, penelitian ini mengandalkan data sekunder dari BSSN, Kominfo, UNICEF, Mafindo, dan literatur ilmiah yang diterbitkan antara tahun 2020 sampai 2025.* ***Pengumpulan data*** *melibatkan analisis tematik untuk mengidentifikasi pola, tren, dan dampak sosial-hukum.* ***Temuan*** *ini mengungkapkan peningkatan kasus dan kerugian yang konsisten, sebagian besar berasal dari penipuan internet dan pelanggaran data.*

Available online at website: https://e-journal.upr.ac.id/index.php/jied

Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

Hukum Islam menganggap kejahatan siber sebagai pelanggaran serius terhadap keadilan, integritas, dan perilaku moral, menekankan peran penting etika digital dan akuntabilitas pribadi dalam lingkungan online. ***Secara unik,*** *penelitian ini menjembatani kesenjangan dalam literatur yang ada dengan menawarkan analisis integratif prinsip-prinsip hukum Islam dan tantangan kejahatan siber kontemporer bidang yang masih kurang dieksplorasi. Penelitian ini menekankan pentingnya mensintesis kerangka peraturan, inisiatif pendidikan, dan standar etika untuk memperkuat keamanan siber. Selain itu, penelitian ini mengadvokasi pengembangan kebijakan berkelanjutan, penggabungan etika agama dalam pendidikan digital, dan peningkatan kerja sama internasional, sehingga memberikan wawasan teoritis dan praktis bagi wacana pencegahan kejahatan siber dalam konteks hukum Islam.*

Kata Kunci: kejahatan siber, hukum Islam, dan tanggung jawab digital

Introduction

Over the past two decades, digital technology has rapidly transformed various aspects of human life, including communication, business, finance, and social interaction. In Indonesia, the daily use of the internet, social media, instant messaging, and other digital platforms has become increasingly prevalent (Azhari, 2021). While digital technology facilitates access to information and communication, it also introduces new vulnerabilities, particularly in the form of cybercrime.

Cybercrime encompasses a wide range of criminal activities involving computers, the internet, and electronic systems. The literature identifies multiple types of cybercrime—such as phishing, online fraud, hacking, identity theft, cyberbullying, and the spread of disinformation or hate speech—with each evolving alongside technological advances (Nugroho, 2020). These crimes present significant challenges for law enforcement, as perpetrators often operate anonymously or from different jurisdictions. Several studies have discussed the legal and technical aspects of cybercrime and its impacts on individuals and society (Rahmatullah, 2019). However, most existing research focuses primarily on positive law and regulatory responses, with limited attention to ethical, moral, and religious perspectives, particularly from the standpoint of Islamic law.

This reveals a research gap: there is insufficient exploration of how Islamic law addresses the ethical and legal dimensions of cybercrime, especially regarding accountability and social responsibility in the digital era. While some scholars have highlighted the importance of moral values in cyberspace, comprehensive analyses integrating Islamic legal principles with the unique challenges of cybercrime remain scarce (Fauzi, 2022).

Therefore, this article aims to (1) identify the forms of cybercrime prevalent in the digital age and (2) analyze Islamic legal perspectives on the ethics and accountability of cybercrime. The novelty of this study lies in its integrated approach, combining the identification of cybercrime types with an in-depth discussion on the application of Islamic law as both a moral and legal framework for addressing cybercrime. This research is expected to enrich the legal scholarship by bridging contemporary cybercrime issues with Islamic ethical and legal values, thereby offering practical guidance for Muslims in the digital era.

Methods

This study employs a qualitative descriptive methodology, using library research techniques

Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

to identify and analyze cybercrime issues in Indonesia. This approach enables the researcher to examine, understand, and analyze empirical data and policies on cybercrime from various secondary sources (Creswell, 2014). The research sources include official reports and data from government agencies, such as the National Cyber and Encryption Agency (BSSN) and the Ministry of Communication and Information Technology (Kominfo), as well as from non-governmental organizations like UNICEF Indonesia and the Indonesian Anti-Fraud Society (Mafindo). Additionally, relevant scientific articles and online news related to cybercrime, its types, tactics, and mitigation efforts (published between 2020 and 2025) were reviewed.

The selection criteria for sources included credibility (peer-reviewed journals or official institutional data), relevance to the themes of cybercrime in Indonesia, and publication date (within the last five years to ensure up-to-date information). Data collection was conducted through systematic searches on public databases, official government and institutional websites, and academic journals.

For the analysis, a content analysis model was adopted (Krippendorff, 2018), involving several stages. First, all collected sources were screened for relevance and credibility. Next, the data were coded thematically based on predefined categories: types of cybercrime, tactics used, regulatory responses, and Islamic law perspectives. Patterns and relationships among variables were identified through iterative coding and cross-comparison between sources. This systematic approach ensured that the analysis was comprehensive, objective, and aligned with the research objectives.

Results

1. Types of cybercrime that are growing as digital technology gets better

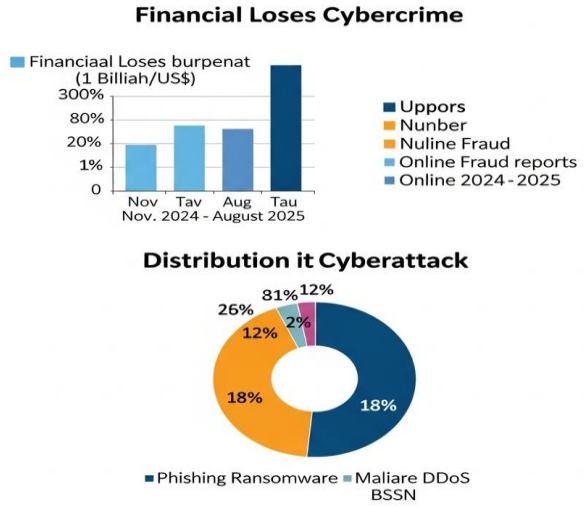
The digital age is especially dynamic because of the rise of information and communication technologies. This progress has made social interactions, business deals, learning, and even government easier, which is a good thing. But the digital era has also made it simpler for cybercrime to happen, which is getting more intricate and tougher to combat with old-fashioned means. Cybercrime is mostly a crime that uses a computer, the internet, or another digital device as a weapon or target (Nugroho, 2020). The National Cyber and Cryptography Agency (BSSN) states that cyber attacks in Indonesia get worse every year, with millions of them of different sizes. In 2022, BSSN saw more than 976 million strange cyber traffic events in Indonesia. Most of these were malware, phishing, and online attacks (BSSN, 2022). This means that cybercrime is now a real danger to the safety of people, businesses, communities, and maybe even the whole country.

a. Fraud on the Internet

Scammers collect sensitive information from their victims in a number of ways, such as selling fraudulent things, fake investments, prize contests, and phishing. The Ministry of Communication and Information says that online fraud was the most common sort of internet crime recorded in 2021 and 2022 (Ministry of Communication and Information, 2022). Recent data shows that there were 1.2 million claims of digital fraud between November 2024 and January 2025, costing Rp476 billion in total (Kominfo, 2025). This type of fraud sometimes uses social engineering, which is when the scammer plays with the victim's mind to get them to give up personal information or send money.

Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

Table 1. Financial Loses Cybercrime



(Source : The BSSN, or National Cyber and Cryptography Agency)

b. Hacking

Hacking is the act of obtaining into, taking, or corrupting data without the owner's consent. In 2021, a big event happened in Indonesia when the personal data of millions of telecom customers was stolen and sold on the dark web (Azhari, 2021). BSSN also said that attacks on the government and vital infrastructure are happening increasingly often. These attacks could be expensive and put the safety of the country at risk (BSSN, 2022).

c. Data Breach

Data leaks happen more and more commonly as more and more digital services gather customer data. People often steal and sell personal information like KTP, NPWP, medical records, and even financial information to perform crimes like identity theft and illegal internet loans. There were a lot of major things that happened between 2021 and 2022, like the Social Security Agency for Health data breach that affected more than 279 million people (Kominfo, 2022). Most of the time, this kind of data leak happens because the security system isn't robust enough and the people using it don't know how to utilize it.

d. Bullying that happens online

Bullying that happens online Digital bullying, often called cyberbullying, is when someone uses digital media to threaten, insult, or spread false information about someone else. A UNICEF research from 2021 says that 45% of Indonesian teens have been bullied online. The effects can be quite bad for your mental health, make you feel alone, and even make you think about killing yourself. People can conduct things in the virtual world without worrying about being discovered out since they are anonymous (UNICEF, 2021).

e. Hoax, changing information, and hate speech

In the age of the internet, distributing false news (hoaxes), wrong information, and hate speech has become a big problem. Deepfake technology can even change pictures and videos, which makes it even harder to tell what's real and what's not. The Indonesian Anti-Fake News Society

Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

(Mafindo) reports that there were around 2,000 hoaxes that were widely shared on social media in 2021 (Mafindo, 2022). Hoaxes and hate speech can make people angry with each other, make the political climate worse, and ruin the reputations of persons and groups.

f. Other Crimes

Other Crimes Cybercrime also encompasses crimes against kids (including grooming and online sexual exploitation), digital money laundering, online extortion (sextortion), and ransomware assaults that lock victims' files and ask for money. As technology becomes better, cybercrime is becoming more complicated and varied. It is increasingly harder to tackle cybercrime because criminals utilize encryption and anonymous networks to commit crimes across borders, which makes it harder for the authorities to apprehend them. Not enough people know about digital security and how to use digital technologies (Fauzi, 2022), which makes things worse. Because of this, fighting cybercrime needs more than just good laws. It also needs moral, educational, and international collaboration (Fauzi, 2022).

2. Islamic Law's Perspective on Cybercrime from an Ethical and Accountability Standpoint

Islamic law is a complete system of regulations that covers all parts of life, including how to pray, work, and act in public. Sharia law emphasizes that whatever a person does, whether in real life or online, must follow the standards of Sharia, which highlight fairness, honesty, responsibility, and the ban on oppression.

a. Ethical Aspects in Islamic Law

Islam stresses morals and ethics (akhlaq) in whatever people do, including when they use digital technology. Principles such as honesty (sidq), trust, fairness, and the prohibition of injuring and disadvantaging others serve as the essential basis for relationships, both conventional and digital (Rahmatullah, 2019). Islamic law places a strong emphasis on morals and ethics (akhlaq) in all aspects of life, including the use of digital technology. Honesty (sidq), trust, fairness, and the prohibition of harming and disadvantaging others are fundamental principles that underpin both traditional and digital partnerships (Rahmatullah, 2019).

Islam forbids lying (gharar), theft, and taking someone's rights in a negative way. There is a reason why QS doesn't allow this. Al-Baqarah: 188 says, *"And do not eat the wealth of others in a way that is not right..."* Hacking and online fraud are clear examples of taking someone's rights without permission, which is against Islamic laws. Al-dharar yuzal is the most essential norm in Islamic law. It says that all kinds of harm must be stopped.

According to Sharia law, hurting someone is not authorized. This includes distributing false information, cyberbullying, and disclosing personal information without authorization. *"You must not put yourself or others in danger,"* said Rasulullah SAW (HR. Ibnu Majah). Islam teaches the idea of tabayyun, which implies checking that the information is correct before spreading it (QS. Al-Hujurat: 6). This is vital for communicating to people and exchanging information on social media. Islamic media ethics believe that spreading lies, hoaxes, and hate speech is wrong.

Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

b. Aspects of Accountability in Islamic Law

In Islamic law, accountability (mas'uliyyah) includes all obligations, both in this life and the next. Every action of a person, even if it happens in the digital realm where no one can see it, is nonetheless recorded and accountable before Allah SWT (Surah Al-Zalzalah: 7-8). In Islam, people who commit cyber crimes must be punished in this life with qishas, diyat, or ta'zir, depending of how terrible the crime was and how much harm it did. In modern contexts, this can be adapted to include criminal sanctions, reparations, or societal repercussions in accordance with applicable statutory provisions (Fauzi, 2022).

Spiritual Responsibility, the person who did the crime must not only face punishment in this life, but they must also repent, say sorry to the victim, and endeavor to fix what they broke. In Islam, taubat means more than merely feeling bad. It also entails doing something to make things right for the victim and promising not to do it again. This fits with the idea of ishlah, which implies peace and progress.

Islamic law lends a lot of weight to the rights of victims. When someone does anything bad online, the victim has the right to be safe, have their rights restored, and get justice. This principle is in line with maqashid syariah, which means protecting religion, life, mind, lineage, and property.

c. The Ulama's Fatwa and Ijtihad

The Ulama's Fatwa says in a number of fatwas that cybercrimes including internet fraud, data theft, and spreading lies through digital media are against the law since they hurt people and violate their rights. Modern scholars also underline that Muslims need to learn how to use technology better and follow media ethics so they don't do things that Sharia bans (MUI, 2020).

d. The combination of Islamic law and positive law

Values like honesty, fairness, and responsibility may make good laws even better. They can also help us develop a safe and healthy digital society. We need to take a full approach to fighting cybercrime. The job of positive law is to punish persons who breach the law, protect victims, and keep the peace in society. Islamic law may help police by teaching individuals about morals, digital ethics, and how to be more responsible in society.

Values like fairness, honesty, the desire to be responsible, and the prohibition of injustice are necessary for a healthy digital culture. This synergy between positive law and Islamic law is expected to decrease cybercrime rates and promote civility in both the digital and physical realms.

This study has comprehensively described the forms of cybercrime prevalent in Indonesia, such as online fraud, hacking, personal data breaches, cyberbullying, disinformation, and hate speech, based on official data and recent literature. However, a critical analysis from the perspective of Islamic law requires deeper exploration beyond normative statements.

From a fiqh perspective, cybercrime can be analyzed through several key principles. For example, the principle of **sadd al-dzari'ah** (blocking the means to harm) justifies prohibiting digital actions that potentially lead to greater harm, such as phishing or online fraud. Similarly, the concept of **al-maslahah al-mursalah** (public benefit) supports the development of preventive measures and regulations to protect public interest in cyberspace. Contemporary scholars, such as Yusuf al-

Copyright © **Muhammad Ruslan Afandi**
Vol. **01**, No. **2**, Desember 2025, Page **261-270**
E-ISSN: 3123-3171
Journal of Islamic Education and Intellectual Discourse (JIED)

Qaradawi and Wahbah al-Zuhayli, emphasize the dynamic application of Islamic law to address new forms of crime, including those in the digital sphere, by prioritizing the protection of life, property, and dignity.

A comparison with other contemporary Islamic legal literature shows that several scholars have begun to address cybercrime within the framework of **maqasid al-shariah** (objectives of Islamic law). The five primary objectives protection of religion (hifz al-din), life (hifz al-nafs), intellect (hifz al-'aql), lineage (hifz al-nasl), and property (hifz al-mal) can all be threatened by cybercrime. For instance, hacking and fraud directly violate the protection of property, while cyberbullying and hate speech may infringe on the protection of dignity and intellect. Thus, Islamic law not only obligates Muslims to avoid such acts but also mandates collective action to prevent and address them.

Despite this framework, the practical implementation of Islamic legal principles in Indonesia's digital policy remains limited. There is a need for further integration between state law, digital literacy initiatives, and religious guidance from Sharia institutions. This aligns with the recommendations of contemporary Islamic jurists and global fatwa bodies, which stress the urgency of contextualizing Islamic values in ever-evolving digital environments.

This study is limited by its reliance on secondary sources and the scope of literature reviewed, which may not cover all perspectives within the diverse field of Islamic law. The analysis focuses on the Indonesian context and may not fully represent the approaches adopted in other Muslim-majority countries. Additionally, empirical data on the practical integration of Islamic legal principles into digital policy and law enforcement is still limited, highlighting the need for further interdisciplinary and field-based research.

Discussion

The study's results show that cybercrime in Indonesia gets worse every year, both in terms of the quantity of crimes and the damage they produce. In 2022, the Cyber and Sandi Negara Agency (BSSN) estimates there were more than 976 million problems with cyber traffic. Most of these events involved malware, phishing, and attacks on the web (BSSN, 2022). Nugroho's view that digital gadgets and the internet are now the main tools or targets of cybercrime in the digital age is supported by this fact.

Reports of digital fraud and losses of Rp476 billion in just three months back up what Kominfo (2022; 2025) found: online fraud is the most widespread sort of cybercrime. The deceptive methods correspond with recognized patterns of social engineering analyzed in previous studies, encompassing the psychological manipulation of victims using social media to unlawfully acquire personal data or financial assets (Kominfo, 2022). This study confirms Azhari's findings, which underscore the significant risks of hacking or data breaches in Indonesia, where incidents of consumer data leaks from telecommunications companies reveal severe vulnerabilities in the national digital infrastructure.

The increasing number of data breaches, as shown by the 2021 Social Security Agency for Health incident, also shows how important it is to improve data security systems and protect user privacy (Kominfo, 2022). UNICEF discovered that 45% of Indonesian adolescents had experienced

cyberbullying. This shows that the psychological and social repercussions of cybercrime are just as important as the economic and security effects.

It is now much tougher to deal with fake news, hoaxes, and hate speech because of deepfake technology. The Mafindo study of 2,000 hoaxes on social media indicates that cybercrime is an issue for more than just people; it also undermines the stability of society and politics. This aligns with Fauzi's research findings, which underscore the necessity for cross-sector solutions that encompass not only advantageous legal frameworks but also the advancement of digital literacy and societal ethics.

The implications of these data indicate that addressing cybercrime necessitates a comprehensive approach. Positive law, encompassing the ITE Law and law enforcement activities, has already laid the groundwork for formal sanctions and protections. Fauzi's study and the results of this study both demonstrate that a moral, educational, and cross-national cooperation approach is necessary to make society more resilient to cybercrime. Digital ethics and education has to be included into the educational system and public campaigns to foster awareness and accountability in the digital domain. These findings support the idea that cybercrime will always change as technology does, so strategies to stop it must be flexible and work together (Nugroho, 2020; BSSN, 2022).

Conclusions

This report highlights that cybercrime in Indonesia continues to escalate, both in frequency and impact. Crimes such as online fraud, hacking, personal data breaches, cyberbullying, disinformation, and hate speech represent significant threats to individuals, communities, and national security. Data from BSSN, Kominfo, UNICEF, and Mafindo show that cybercrime in Indonesia is a highly complex issue requiring multifaceted solutions.

Findings from this study confirm that combating cybercrime cannot rely solely on legal measures. Instead, a comprehensive approach that integrates legal enforcement, education, moral values, and cross-sectoral collaboration is essential for cultivating a safe and resilient digital culture. The integration of Islamic legal principles—such as justice, honesty, and social responsibility—into digital policy and education can significantly strengthen societal resilience against cybercrime. This synthesis of empirical evidence and Islamic legal norms demonstrates that fostering digital literacy and moral awareness is critical for effective prevention and mitigation.

Theoretically, this study contributes by offering an integrated framework that aligns empirical findings on cybercrime with Islamic legal and ethical perspectives, thus filling the gap in the current literature. For policymakers, these findings underscore the need to develop digital policies that emphasize not only law enforcement but also moral education and the inclusion of religious values as preventive measures. Sharia institutions can play an active role in promoting digital ethics and accountability among Muslims, supporting educational initiatives, and providing guidance on responsible online behavior. For the general public, especially the younger generation, this research highlights the importance of digital literacy and ethical conduct as personal and collective responsibilities in the digital era.

Future research could explore the effectiveness of digital literacy programs, the practical integration of Islamic legal principles into national cybersecurity strategies, and interdisciplinary

approaches for enhancing international cooperation in cyber law enforcement and data protection. Practically, the results of this research can serve as a reference for policymakers, educators, and the wider public in both preventive and repressive efforts to address the increasing threat of cybercrime in Indonesia.

Acknowledgment

The author expresses gratitude to the Indonesian Cyber and Sandi Negara Agency (BSSN), the Indonesian Ministry of Communications and Information (Kominfo), UNICEF Indonesia, and the Indonesian Anti-Fitnah Society (Mafindo) for the figures, reports, and information that greatly aided in the composition of this essay. The author also acknowledges the place where he or she works for giving them the option to go to seminars and talks about cyber security issues, as well as emotional support and other resources. The author also thanks coworkers who supplied helpful feedback and suggestions for how to improve this post.

References

Badan Siber dan Sandi Negara (BSSN). (2022). Statistik Insiden Siber Indonesia 2022. https://bssn.go.id/statistik/

Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). (2022). Laporan Aduan Masyarakat Terkait Kejahatan Siber. https://kominfo.go.id/

Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). (2025). Kerugian Penipuan Digital Capai Rp476 Miliar, 1,2 Juta Laporan Masuk. https://portal.komdigi.go.id/kanal-publik/berita-kini/9525

Nugroho, W. (2020). Kejahatan Siber: Teori, Praktik, dan Regulasi di Indonesia.

Azhari, M. (2021). Kebocoran Data Telekomunikasi dan Tantangan Cybersecurity. Tirto.id.https://tirto.id/kebocoran-data-telkomsel-indikasi-seriusnya-kejahatan-siber-di-ri-ghrA

UNICEF. (2021). Cyberbullying in Indonesia: Youth Perspectives. https://unicef.or.id/cyberbullying

Masyarakat Anti Fitnah Indonesia (Mafindo). (2022). Laporan Tahunan Hoaks 2021. https://turnbackhoax.id/

Fauzi, A. (2022). Penanggulangan Kejahatan Siber: Pendekatan Moral, Edukatif, dan Kerja Sama Lintas Negara.

Sejati, Y. D. C., & Nugroho, M. A. S. (2023). Upaya peningkatan kompetensi penyidik Direktorat Tindak Pidana Siber Bareskrim Polri dalam menangani kasus cyber crime. Jurnal Riset Manajemen Akuntansi Indonesia, 1(2), 380–408. https://doi.org/10.32477/jrima.v1i2.699

Koprawi, M., & Nugranto, H. F. (2024). Investigasi Kejahatan Siber pada Surface Web dan Deep Web Menggunakan Metode NIST. JATISI, 11(1). https://doi.org/10.35957/jatisi.v11i1.3245

Setiawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Upaya Regulasi Teknologi Informasi dalam Menghadapi Serangan Siber (Cyber Attack) Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. Jurnal USM Law Review, 3(2), 275–295. https://doi.org/10.26623/julr.v3i2.2773

Rumapea, C. P., & Puspitasari, M. (2023). Kejahatan Siber di Indonesia pada Masa Pandemi Covid-19: Ancaman dan Pencegahan dalam Kajian Intelijen Strategis. Syntax Literate: Jurnal Ilmiah Indonesia, 7(10). https://doi.org/10.36418/syntax-literate.v7i10.12558

Pramono, A., Musarofah, A., Rohmah, A. N., Saputra, A., & Abdullah, H. F. (2025). Sosialisasi Keamanan Cyber dan Bahaya Judi Online. Jurnal Pengabdian Masyarakat Bangsa, 3(8), 3893–3898. https://doi.org/10.59837/jpmba.v3i8.3188

Syahrian, M. R., & Nugroho, W. C. (2025). Tinjauan yuridis mengenai kekerasan pada perempuan dalam kejahatan cybercrime. Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 3(1). https://doi.org/10.53363/bureau.v3i1.216

Kusumawaty, I., Yunike, Y., Elviani, Y., & Arifin, H. (2021). Contributing factors of cyberbullying behavior among youths during Covid-19. Jurnal Ners, 16(1). https://doi.org/10.20473/jn.v16i1.24751