LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 14, No. 5, 2025, pp. 1141-1150
Published by: IHSA Institute (Natural Resources Law Institute)

Cybercrime digital crime how technology is utilized for crime

M. Nassir Agustiawan[1], Arif Budiman[2], Dian Samudra[3]

[1,2,3]Faculty of Law, Bina Bangsa University, Serang, Banten

Abstract: The rapid development of digital technology has brought positive impacts in various aspects of life, such as communication, economy and education. However, on the other hand, this progress also opens up opportunities for various forms of digital crime or cybercrime. Digital crimes include various criminal acts committed through the internet and technology, such as hacking, identity theft, online fraud, malware distribution, and exploitation of personal data. This study aims to understand how technology is utilized to commit crimes in cyberspace, the factors that drive digital criminals, and the implications faced by victims and the wider community. In addition, this study will also discuss strategies and efforts that can be made to prevent and tackle digital crime. With the increasing reliance on technology, it is important for society and legal authorities to be more vigilant and proactive in addressing this challenge. An in-depth understanding of the modus operandi of digital criminals is expected to provide a clearer picture for the development of effective cybersecurity policies.

Keywords: CyberCrime; Education Technology; Social Media.

1. Introduction

The most specific research gap in this article lies in the lack of previous studies that simultaneously integrate digital technology developments, security system vulnerabilities, perpetrator motivations, and legal and policy responses within a single, comprehensive analytical framework. Unlike previous research, which tends to be fragmented around the modus operandi or regulatory aspects alone, this article offers a novelty through an interdisciplinary approach that links the technological dimensions, criminal behavior, and governance of cybercrime prevention policies. The development of digital technology has brought fundamental changes to the way people communicate, transact, and manage information. The digitization of public services, financial systems, e-commerce, and the use of social media and cloud computing have created a vast and interconnected cyberspace. However, despite the benefits of efficiency and accessibility, technological developments have also opened up new opportunities for cybercrime. The complexity of digital systems, dependence on internet networks, and the speed of technological innovation are often not matched by adequate security preparedness. Security system vulnerabilities are a key factor bridging the gap between technological development and cybercrime. These vulnerabilities can stem from software weaknesses (bugs, security vulnerabilities), poor system configuration, weak passwords, lack of system updates, and low user digital security literacy. In many cases, the human factor is the weakest point in security systems, for example through phishing or social engineering practices that exploit user trust and negligence.

The motivations of cybercriminals also determine how these vulnerabilities are exploited. The perpetrators' motivations are diverse, ranging from economic (financial gain), political and ideological (hacktivism, cyber espionage), organized crime, to personal motives such as revenge, intellectual challenge, or the search for recognition. These motivations influence the complexity of the attack, the targets chosen, and the methods used by the perpetrators in carrying out their actions. The interaction between digital technology developments, security system vulnerabilities, and perpetrators' motivations ultimately gives rise to various forms of cybercrime. These forms include online fraud,

Correspondence:
Name: M.Nassir Agustiawan
Email: mukhamadnassiragustiawan@gmail.com

Received: Nov 30, 2025;
Revised: Dec 09 2025;
Accepted: Dec 20, 2025;
Published : Dec 30, 2025

identity theft, hacking, the distribution of malware and ransomware, crimes against personal data, attacks on critical infrastructure, and the misuse of social media for disinformation and hate speech. Cybercrime is dynamic and adaptive, with perpetrators continually adapting their criminal techniques to the latest technology and existing defense patterns. Thus, the conceptual framework of cybercrime can be understood as a causal and interactive relationship: digital technology developments create new opportunities and spaces, security system vulnerabilities provide exploitable loopholes, perpetrators' motivations drive criminal acts, and the interaction of the three results in various forms of cybercrime. This framework emphasizes that cybercrime prevention efforts must not only focus on technological aspects, but must also include strengthening security governance, increasing digital literacy, and law enforcement that is adaptive to the dynamics of cyberspace.

In an increasingly integrated digital era, information and communication technology plays a crucial role in everyday life. The development of the internet and digital devices not only facilitates social interaction, commerce, and access to information, but also opens up new opportunities for crimes that utilize technology. The phenomenon of digital crime, also known as cybercrime, covers a wide range of illegal activities conducted in cyberspace. These activities include hacking, data theft, online fraud, ransomware, and other cyberattacks that often aim to harm individuals, companies, or even countries. Digital crimes have unique characteristics as they often cross national borders, are difficult to detect, and perpetrators can operate anonymously(Irawati et al., 2021). This causes great challenges for law enforcement and relevant authorities in detecting, arresting and punishing perpetrators. In addition, digital criminals continue to develop new and increasingly sophisticated methods, capitalizing on weaknesses in digital security systems as well as the lack of public understanding of cyber risks. Meanwhile, the impact of digital crime can be devastating, both financially and psychologically, especially when it involves personal or confidential data. This introduction will examine how technology is being used for cybercrime, the factors contributing to the rise in digital crime, and the need for stronger cybersecurity awareness and policies. This research is expected to provide insights into the modus operandi of digital criminals and the importance of digital protection in the face of evolving threats(Aji, 2023).

Digital crime or cyber crime is a criminal act that involves computers, network devices, or the internet as a tool, target, or environment to carry out illegal activities. Along with the rapid development of technology, digital crime is increasingly prevalent and develops in various forms, ranging from hacking, identity theft, online fraud, to the spread of malware. These types of crimes can harm individuals, organizations, companies, and even countries. Here are some common forms of digital crime Hacking Hacking is the act of entering a computer system or network without authorization to steal, alter, or destroy data. Hackers often exploit weaknesses in security systems to gain unauthorized access(Ummah, 2019). Identity Theft This occurs when a perpetrator steals personal information, such as identification numbers, credit card information, or passwords, for the purpose of defrauding or gaining financial gain on behalf of the victim. Phishing This involves fraud perpetrated through fake emails, text messages, or websites created to trick victims into providing personal or financial information. Online Fraud This crime includes various forms of fraud, such as buying and selling fictitious goods on e-commerce sites, fake investment offers, or ponzi schemes run online(Prasetiyo & Zuhdy, 2020). Malware and Ransomware Malware is malicious software designed to damage or access computer systems without authorization. Ransomware, a type of malware, locks the victim's data and demands a ransom for the data to be returned. Cyberstalking and Cyberbullying This form of crime involves intimidation, threats or harassment through digital platforms. Cyberstalking usually takes the form of online stalking, while cyberbullying is more related to harassment on social media or messaging apps. Spread of Illegal Content Digital crime also includes the spread of illegal content, such as child pornography, hate speech or terrorist propaganda over the internet. The Impact of Digital Crime Digital crime can result in significant financial losses, especially

for businesses hit by cyberattacks or individuals who fall victim to fraud. In addition to economic losses, digital crime also poses a threat to the privacy and security of personal data, which can cause psychological and emotional impacts for victims. At the national level, cyberattacks on critical infrastructure, such as power grids or financial systems, can threaten the stability and security of the country. Prevention and Countermeasures To prevent digital crime, it is important for individuals and organizations to raise awareness about cyber threats and implement good security practices. Some steps include Strengthening Password Security Using strong and unique passwords for each account, and enabling two-factor authentication.

Install Security Software Antivirus and anti-malware can help protect. (Febriani Wardojo, 2018) your device from common threats. Update Software Regularly System and application updates usually include fixes for security vulnerabilities. Beware of Phishing Check the source of emails or links before providing personal information or clicking on suspicious links. Educate Yourself on Cybersecurity Training and education on cybersecurity can help individuals and organizations be more aware of threats. In addition, governments and law enforcement authorities have an important role to play in tackling digital crime through strict regulations, international cooperation and the development of security technologies. With strong collaboration between the public, private and community sectors, digital crime threats can be tackled more effectively(Noor et al., 2022).

Cybercrime or digital crime is one of the most significant security challenges in today's digital age. Technology is often utilized by perpetrators to carry out various criminal acts, such as identity theft, online fraud, malware distribution, and cyberattacks on critical infrastructure. These crimes not only cause losses to individuals and companies, but also threaten national security. In this context, the government has a very important role in prevention, mitigation, and law enforcement efforts related to digital crimes. Policymaking and Regulation The government needs to formulate and strengthen laws and regulations related to digital crime. For example, laws related to data protection, privacy, and cybersecurity. Creating clear and detailed policies will help regulate online activities and provide a legal basis for dealing with digital criminals(Kurniawan & Hapsari, 2021). Regulations should cover various aspects, including hacking, malware spread, data theft and illegal content dissemination. Improving Cybersecurity Infrastructure The government needs to invest resources in the development of a robust cybersecurity infrastructure to protect critical data and systems from cyberattacks. The establishment of a national cybersecurity operations center can help in effective monitoring, early detection and response to cyber threats. The government can work with technology companies and internet service providers to strengthen security protocols, especially to protect vital infrastructure such as power grids, banking and healthcare(Idhel et al., 2024). International Cooperation As digital crime is cross-border in nature, international cooperation is necessary to effectively address the issue. Governments can work with other countries, international organizations, and law enforcement agencies to track and crack down on digital criminals. Participation in international treaties, such as the Budapest Convention on Cybercrime, as well as exchanging information and countermeasure strategies with other countries, can strengthen efforts against digital crime(Widodo, 2016).

Public Education and Awareness The government has an important role in educating the public about the risks and preventive measures against digital crime. Socialization programs and public awareness campaigns can help people understand cyber threats and how to protect themselves. Education can also be aimed at businesses to improve their understanding of cybersecurity, as well as the importance of protecting customer data. The government can encourage cybersecurity training in schools, universities and workplaces so that more people have a basic understanding of digital security. Law Enforcement and Investigation The government, through law enforcement agencies, has the responsibility to investigate and prosecute digital criminals. This requires specialized units trained in cyber investigation and digital forensics(*Juridical Review of Sundanese Traditional Marriage and Its Recognition in National Law*, 2024). The government can facili-

tate specialized training for police and law enforcement on how to track digital criminal activity, analyze digital evidence, and present this evidence in court. Effective law enforcement requires collaboration between the government, law enforcement and the private sector to share information and resources in an effort to catch cybercriminals. Security Technology Development and Research The government can fund research and development of cybersecurity technologies to continuously update ways to deal with new threats. For example, the development of artificial intelligence and algorithms capable of automatically detecting anomalies or attacks. Collaboration with research institutions and universities can encourage innovation in the field of cybersecurity, as well as produce new solutions that can be used to detect and mitigate cyber threats(Siahaan, 2018). Providing Assistance and Recovery for Victims In addition to prevention efforts, the government also has a role in helping victims of digital crime. The government can provide assistance and recovery services for those who are victims of fraud, identity theft, or other cyber attacks. The government can work with legal aid organizations to provide victims with access to the information, resources, and support needed to recover from losses due to digital crime. Through a comprehensive and sustainable approach, the government's role in fighting digital crime can be more effective. With strong regulations, international cooperation, and increased public awareness, it is hoped that prevention and law enforcement efforts against digital crime can work well, and reduce the negative impacts they cause(Agustiawan et al., 2024).

2. Materials and Methods

The criteria for selecting secondary data sources were based on the credibility of the publisher (reputable journals, official cybersecurity institutions, and international organizations), the novelty of the publication, the clarity of the methodology and the validity of the data used. Furthermore, substantive relevance was a primary consideration, namely the suitability of the literature and reports to the focus of the cybercrime study, the context of the digital technology being analyzed, and their relevance to the conceptual framework and research objectives. In this section, we describe the approach, data and methods used to understand how technology is used to commit digital crimes. The research used a qualitative approach that involved analyzing secondary data from various sources, including scientific literature, cybercrime reports, and interviews with cybersecurity experts. The focus of this research method is to identify common modus operandi in digital crimes, understand their impact, and examine prevention and countermeasure strategies implemented by relevant parties. Data Collection Scientific Literature and Case Studies: Data was collected from scholarly articles, journals, and case studies that address different types of digital crime, such as hacking, phishing, malware, and online fraud. These sources provide an understanding of the technologies used by digital criminals and the common patterns they follow. Cybersecurity Reports: Secondary data is drawn from annual reports published by global cybersecurity agencies and major technology companies. These reports cover cyberattack trends, loss statistics, and methods used by digital criminals.Expert Interviews: Semi-structured interviews were conducted with cybersecurity experts, law enforcement, and practitioners in the information technology field. These interviews aimed to gain insight into the challenges faced in preventing digital crimes as well as the strategies implemented to address these threats.Case Law(Suci Meinarni & Sari, 2020) Data from legal cases related to digital crimes were also analyzed to understand how these crimes are dealt with legally. This information includes relevant laws, law enforcement procedures and court outcomes(*Juridical Review of Sundanese Traditional Marriage and Its Recognition in National Law*, 2024).

3. Results and Discussion

Cybercrime law enforcement currently faces limited human resource capacity with digital forensic expertise, disparities in capabilities between specialized units, and investigative procedures that are not yet fully adapted to the complexity and speed of cybercrime.

Furthermore, case studies demonstrate obstacles to proving evidence in court, particularly regarding the validity of electronic evidence, the chain of custody, and differing legal interpretations of technology-based crimes. This article proposes multi-stakeholder collaborative partnerships through the exchange of cyberthreat information, integration of incident reporting systems, and the development of mutually agreed-upon security and incident response standards between the government, the private sector, and internet service providers. Furthermore, synergy with law enforcement agencies and civil society is strengthened through increased digital forensic capacity, public cybersecurity literacy, and transparent and accountable law enforcement mechanisms. Research on digital crime shows that technology has been utilized in various forms to commit crimes in cyberspace. Some of the key findings from this research reveal how technology is used by perpetrators to exploit systems, gain financial benefits, and launch attacks against individuals or organizations. Below we discuss the key results relating to the modus operandi of digital crime, its impact, and the prevention and countermeasures that can be taken.Modus Operandi in Digital Crime Digital criminals make creative use of technology to achieve their goals. Some of the main modus operandi include Hacking and Exploitation of System Vulnerabilities Many cyberattacks occur due to gaps or vulnerabilities in security systems. Hackers often use automated software to scan networks and find weak points that can be exploited. These attacks can be SQL Injection, Brute Force, or DDoS (Distributed Denial of Service) attacks. Phishing and Social Engineering: Cybercriminals often use phishing and social engineering techniques to manipulate victims into providing their personal information. In some cases, emails or text messages are sent with a convincing appearance to get victims to click on fake links and enter their login data, credit card numbers, or other sensitive information. Malware and Ransomware Distribution Malicious software such as malware and ransomware are used to corrupt or access data without authorization. Ransomware, in particular, encrypts the victim's data and demands a ransom payment to unlock it. Ransomware attacks have increased rapidly, especially on healthcare, education, and government institutions. Online Fraud and Fake Investment Schemes Digital crime also involves various forms of financial fraud, including fake investment schemes, fake trading websites, and offers that are too good to believe. By utilizing social media platforms, perpetrators can target victims widely and quickly(Hukum et al., 2016).

Impact of Digital Crime Digital crime has far-reaching impacts on individuals, organizations, and society. These impacts include Financial Losses Many individuals and companies experience substantial financial losses due to digital fraud, data theft or ransomware. According to recent reports, global losses due to digital crime are estimated to be in the billions of dollars each year. Reputational Loss: For companies, especially those with large customer databases, cyberattacks can cause loss of customer trust and damage reputation. For example, a leak of customer data can result in a loss of trust and lower the value of the company. Threats to Privacy and Security: Personal data breaches and identity theft are very serious issues. Individuals who experience identity theft may face legal and financial problems due to the misuse of their data by criminals and cyberbullying. Many victims experience stress, anxiety, and trauma as a result of the threats or intimidation they experience online. Prevention and Countermeasures The results of this study also show that there are several important steps that can be taken to prevent and address digital crime, including Raising Public Awareness and Education Public awareness of the risks of digital crime is still low. Therefore, education about cybersecurity is needed at the individual, organizational and government levels. Cybersecurity education programs should be introduced in schools, workplaces, and communities. Security Technology Development Cybersecurity technologies, such as encryption, firewalls, and anti-malware software, play an important role in protecting data and networks from attacks. The development of artificial intelligence (AI)-based technologies can also help in automatically detecting and responding to cyber threats. Improved Regulations and Policies The government needs to develop stricter regulations related to data protection and cybersecurity. In addition, international collaboration in law enforcement is essential

as digital crimes are cross-border in nature. Rapid Response and Incident Handling Organizations need to have a rapid response team to cyber incidents and a recovery plan. These teams should be trained in handling cyberattacks and be able to recover data or systems quickly to minimize losses.Inter-Sector Cooperation Countering digital crime requires collaboration between the government, private sector, law enforcement, and the general public(Madinah Mokobombang et al., 2023). This includes information exchange, resource sharing, and joint strategies to prevent and address digital crime.

Discussion These results show that technology has become a very effective tool for digital criminals. However, technology can also be used as a solution to protect ourselves and prevent crime. The use of artificial intelligence, machine learning, and data analytics can help in detecting suspicious behavior patterns and preventing cyberattacks before they happen. Public awareness and good policies from the government are also important to reduce the risk of digital crime. Governments, educational institutions, and the private sector need to work together to continuously develop innovative cybersecurity solutions. Public education and awareness should be prioritized so that people are more responsive to cyber threats and can proactively protect themselves. In conclusion, while digital crime is a complex and evolving challenge, with a comprehensive and collaborative approach, this threat can be effectively managed and minimized(W et al., 2024).

The Positive Side Social media is currently a tool that cannot be abandoned in life. Every individual needs social media because every individual in social relationships definitely needs other individuals as friends to interact with. Social media helps a person in carrying out their daily activities, whether consumption for personal, family, group, organization, etc. The benefits of social media as a means of learning, listening, and communicating. Along with the times, the learning process has undergone a very significant change where in the past we learned using the means of blackboards and chalk today is no longer known, everything has changed. Social media can be used for learning tools such as finding learning information, language courses, online lectures, and even finding the desired job. Besides that, social media can also be used to find friends, mates both in the real world and in cyberspace(Febriani Wardojo, 2018).

Documentation, Administration, and Integration Tools. The second use of social media is as a function of documentation, administration, and integration. Social media applications are basically a place for you to store various content, ranging from profiles, information, reportage, events, event records, to the results of research studies. Besides that, social media can also create an Organizational Blog, integrate various lines in the company, disseminate relevant positive content according to public demand and as an effective medium in the operation of an organization(Madinah Mokobombang et al., 2023).

Planning, Strategy, and Management Tools Next is the use of social media as a means of planning, strategy, and management. A management expert will use social media as a marketing tool for products to be marketed, social media is the most powerful weapon to promote, plan strategies in attracting customers, exploring market share, educating smart prospective buyers and getting input from collecting opinions/responses(Eka Sila & Mochamad Taufik, 2023).Promoting, planning strategies in attracting customers, exploring market share, educating smart prospective buyers and getting input from collecting opinions / responses from consumers or from the public about the products needed. Means of Control, Evaluation, and Measurement. The last benefit of social media is that it can be used for control, evaluation and measurement functions. The control function of an organization and the evaluation function can increase the role of the organization in the midst of society. Both in planning and strategizing. What is meant as a measuring tool is measuring public satisfaction with a particular product or measuring public responses about the performance of an organization as well as evaluating its strengths and weaknesses(Ekawati, 2018).

The Negative Side The rapid development of technology will have a domino effect, where crimes will arise by utilizing digital technology for certain purposes. Information technology will facilitate unlimited relationships so that communication can be done

anywhere and anytime without being limited by space and time. Evil intentions will be facilitated by versatile devices such as: Face book, Instagram, WhatsApp, email etc. Social media is easily used for malicious purposes online regardless of time, target, status which will cause material and immaterial losses. Perpetrators can commit individually or in groups for a crime. Factors that cause Cyber Crime Security System Vulnerabilities or gaps in the security system make it easier for people to access and commit cyber crimes, so social media must always be routinely checked to protect the evil actions of irresponsible people. Cyber crime is very easy to commit. Lack of Security Awareness Do not just click on links without understanding the security risks, do not easily accept calls from unknown numbers, especially from people who call without a name. Ignore calls from people promising prizes that you don't know the origin of, or don't answer if you don't think you're participating in a prize draw(Ginara et al., 2022).

Technological Advancements Rapid technological advancements provide many benefits while opening the door to cybercriminals. Anonymity on the Internet Cyber criminals have the motivation or opportunity to commit crimes because of the convenience obtained from the internet, even criminals can easily hide their personal identity without being traced and do not feel afraid of legal sanctions or risks that ensnare them. Even if the perpetrator is known, it will take a long time to catch him, because crimes like this can be committed across countries. Human Exploitation (Social Engineering) Social engineering techniques can allow cybercriminals to often manipulate individuals or employees into providing confidential information or accessing secure systems. Social engineering techniques can be more successful and easier to perform. Lack of Firm Punishment Weak existing laws make cyber criminals not afraid of being caught or punished, because these types of crimes are difficult to track(Monika & Monita, 2023). Dependence on Technology The dependence of organizations or individuals on digital technology will increase the potential for cyberattacks, because technology is already a part of everyday life. In the current digitalization era, it is difficult for people to live without interacting with each other, incoming information is always an inseparable part of life. People will easily know the situation and conditions in a place, both regions and countries anywhere in the world(Septasari, 2023).

User Identity The ease of providing personal identity will open up opportunities for people to do bad things. There are many features that provoke people to know their identity so that people will easily provide their personal identity without thinking about the risks they will receive. With sweet seduction, someone will be tempted to provide personal identity, both the Population Identification Number, name and current address. Replication of Information Assets Social media activists can easily replicate or duplicate information assets. Deleted information can be easily restored or reappeared, because the internet system does not recognize the name "Delete Button". Location The next cybercrime is that your location can be easily detected on social media. So that criminals can freely know the whereabouts of a person and easily intimidate people who will be targeted for fraud or crime Financial Motivation The goal or target of cyber crime is due to money or financial motivation, the perpetrator will try to get as much money as possible in various ways, both persuasively and with threats that in the end the goal is achieved. Money or finance is the main target because this kind of crime is easy to obtain without the need to work hard(Chintia et al., 2019). Dynamic Digital Environment Social media crime by utilizing digital technology (Internet) is very dynamic and easy to move. This is what is difficult to track because cyber criminals can know when their crimes begin to be detected by the legal apparatus, with the swiftness of cyber criminals moving their hardware to a new area easily and quickly(Vogen L. M. T. Mantik, 2022). Types of Cyber Crime in the Digital Era The current digital system provides an opportunity to commit crimes that use information technology is increasingly rampant and develops without being detected easily, with the sophistication of communication tools various things can be done for the right or wrong purpose. CyberCrime is very dangerous because it has the potential to damage personal or group data that will destroy the economy, business, infrastructure and damage the stability of state security. On the one hand, to prevent the

spread of cyber crime, cyber security has not been able to counteract and prevent crimes that use sophisticated and modern tools because cybersecurity is still far inferior to the tools used by cyber criminals(Dermawan et al., 2023).

Electronic Transaction Information Law (ITE Law). To be honest, it has not been reliable in preventing cyber crimes that are increasingly sophisticated in terms of digital world crimes. Unauthorized access, a type of cybercrime that involves infiltrating a computer system without permission. Examples of well-known crimes are Trujan and Ransomware, which infiltrate viruses to damage computer data(Hilmi et al., 2018).

4. Conclusions

Theoretically, this article contributes by developing an integrative analytical framework that connects the dynamics of digital technology, cybercrime patterns, and legal and policy responses, thereby enriching the body of cybersecurity and law studies in developing countries. Practically, the findings of this article provide strategic recommendations for Indonesia in strengthening regulations, enhancing the capacity of law enforcement officers, and developing multi-stakeholder collaboration to build adaptive and sustainable cybersecurity governance. Future research is recommended to examine cybercrime using an empirical approach through field studies, big data analysis of cyber incidents, or cross-country comparisons to obtain a more contextual and measurable picture. Furthermore, future research could expand its focus to include regulatory effectiveness, institutional readiness, and the role of artificial intelligence in cybercrime prevention and detection. Digital crime has become a serious threat in the era of advanced information technology. Technology not only facilitates daily life, but is also utilized by criminals to launch various criminal acts in cyberspace. Some of the main modes of digital crime include hacking, phishing, malware distribution, and online fraud. These modes not only cost individuals and organizations financially, but also pose threats to privacy, reputation and security. The impact of digital crime is wide-ranging, from financial loss to loss of public trust to risks to national security. Given the cross-border and evolving nature of these crimes, the challenges in tackling them are increasingly complex. Therefore, it is crucial that the government, private sector and communities work together to counter this threat. Some effective prevention measures include public awareness and education, cybersecurity technology development, and strong law enforcement and international cooperation. With coordinated and continuous efforts, risks from digital crime can be minimized, and cybersecurity can be strengthened. In addition, it is important for individuals and organizations to be vigilant and proactive in protecting their data and maintaining their privacy online. In conclusion, while digital crime continues to evolve as technology advances, through a comprehensive approach involving all stakeholders, this threat can be dealt with more effectively and prevent greater harm to society as a whole.

Acknowledgments: The author would like to thank the rector of the University of bina bangsa Prof. Dr. Ir. H. Furtasan Ali Yusuf, S.E., S.Kom., M.M who has motivated lecturers to race to produce scientific writing that can be useful for many people.

References

Agustiawan, M. N., Samudra, D., & Hifni, M. (2024). *Juridical Analysis of the 2024 Simultaneous Regional Elections in Realizing Regional Autonomy in Indonesia*. *13*(2), 298–304.

Aji, B. B. (2023). Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. *Cyber Security Dan Forensik Digital*, *6*(1), 25–29. https://doi.org/10.14421/csecurity.2023.6.1.4049

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati S.Kom., M.Sc.Eng, N. A. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal of Information Engineering and Educational Technology*, *2*(2), 65. https://doi.org/10.26740/jieet.v2n2.p65-69

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank

Indonesia. *Jurnal Informasi Dan Teknologi*, *5*(3), 20–25. https://doi.org/10.60083/jidt.v5i3.364

Eka Sila, G., & Mochamad Taufik, C. (2023). Literasi Digital Untuk Melindungi Masyarakat Dari Kejahatan Siber. *Komversal*, *5*(1), 112–123. https://doi.org/10.38204/komversal.v5i1.1225

Ekawati, D. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan. *UNES Law Review*, *1*(2), 157–171. https://doi.org/10.31933/law.v1i2.24

Febriani Wardojo, M. (2018). *Legal Standing*. *2*(1), 242–255. https://news.detik.com/berita/d-3567290/polling-58-masyarakat-puas-kinerja-kpk,

Ginara, I. G. K., Widyantara, I. M. M., & Styawati, N. K. A. (2022). Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia. *Jurnal Preferensi Hukum*, *3*(1), 138–142. https://doi.org/10.22225/jph.3.1.4673.138-142

Hilmi, R. Z., Hurriyati, R., & Lisnawati. (2018). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*. *3*(2), 91–102.

Hukum, M., Di, P., Aan, O., & Johanes, A. (2016). Pembuktian Terhadap Kejahatan Dunia Maya Dan Upaya Mengatasinya Menurut Hukum Positif Di Indonesia. *Lex Crimen*, *5*(2), 91–99.

Idhel, S., Damanik, W., Prasetio, M. A., Adawiyah, R., Ramadhana, W., & Pra-, J. (2024). *Legal Analysis of Criminal Acts of Corruption of Livestock Budget (Study of Decision No . 3038 K / Pid . Sus / 2021)*. *13*(4), 953–959.

Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. *Prosiding Conference On Law and Social Studies*, 1–15. http://prosiding.unipma.ac.id/index.php/COLaS

Juridical Review of Sundanese Traditional Marriage and Its Recognition in National Law. (2024). *13*(3), 819–827.

Kurniawan, K. D., & Hapsari, D. R. I. (2021). Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah. *Pleno Jure*, *10*(2), 122–133. https://doi.org/10.37541/plenojure.v10i2.590

Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *2*(6), 517–525. https://doi.org/10.58812/jhhws.v2i6.447

Monika, M., & Monita, Y. (2023). Perlindungan Hukum Terhadap Wanita Dari Kejahatan Seksual Secara Online (Cyber Harassment). *PAMPAS: Journal of Criminal Law*, *4*(2), 191–200. https://doi.org/10.22437/pampas.v4i2.26992

Noor, M., Faris, Sidqi, F. A., & Herlina, S. (2022). *Analisis yuridis tentang perlindungan nasabah bank dalam penggunaan short message service (SMS) banking terhadap kejahatan dunia maya*. *4*. http://eprints.uniska-bjm.ac.id/id/eprint/9975

Prasetiyo, P., & Zuhdy, M. (2020). Penegakan Hukum Oleh Aparat Penyidik Cyber Crime Dalam Kejahatan Dunia Maya (Cyber Crime) Di Wilayah Hukum Polda Diy. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(2), 79–88. https://doi.org/10.18196/ijclc.v1i2.9611

Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*, *5*(2), 227–233. https://doi.org/10.30604/jti.v5i2.231

Siahaan, A. P. U. (2018). Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia. *Jurnal Teknik Dan Informatika*, *5*(1), 6–9.

Suci Meinarni, N. P., & Sari, H. B. (2020). Analisis Potensi Kejahatan di Dalam Dunia Maya Terkait Data. *Kertha Wicaksana*, *14*(April 2019), 9–15. https://www.ejournal.warmadewa.ac.id/index.php/kertawicaksana/article/view/1530/1355

Ummah, M. S. (2019). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *Sustainability (Switzerland)*, *11*(1), 1–14. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

Vogen L. M. T. Mantik. (2022). Tinjauan Yuridis Tentang Kedudukan Alat Bukti Digital Dalam Tindak Pidana Kejahatan Mayantara (Cyber Crime). *Lex Privatum*, *10*(5), 1–9.

W, W. O. R., Ahmad, B., & Rusdi, M. (2024). *Analysis of DKI Jakarta ' s APBD Fund Allocation Policy for Improving the Quality of Public Services at the City Level*. *13*(3), 926–935.

Widodo, T. (2016). Pengembangan Model Digital Forensic Readiness Index (DiFRI) untuk Mencegah Kejahatan Dunia Maya. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *1*(1), 41–46. https://doi.org/10.14421/jiska.2016.11-06