MAWADDAH: Jurnal Hukum Keluarga Islam **p-ISSN 3031-5247**
DOI: https://doi.org/10.52496/mjhki.v2i2.169 **e-ISSN 3026-6076**

THE EFFECT OF DIGITAL TECHNOLOGY ON CRIMINAL LAW ENFORCEMENT: AN ANALYSIS OF CYBERCRIME AND ITS HANDLING

Novan Eka Setiyawan[1], Donny Eddy Sam Karauwan[2], Jumiran[3], Abidah Abdul Ghafar[4]
[1-3]Sekolah Tinggi Ilmu Hukum (STIH) Manowari
[4]Associate Professor, Faculty of Syariah and Law, Universiti Sains Islam Malaysia
[*] E-mail Correspondence: novaneka74@gmail.com

Submitted: 21-08-2024	Accepted: 29-10-2024	Published: 05-11-2024

Abstract

This research aims to identify the impact of digital technology development on criminal law enforcement, especially in the context of cybercrime. The research uses a normative juridical method with a literature analysis approach (library research), which includes a review of laws and regulations, court decisions, and case studies related to cybercrime. The results show that digital technology has facilitated significant changes in the modus operandi of cybercrime, ranging from phishing to attacks using artificial intelligence (AI) and cryptocurrency, which complicates law enforcement. The contribution of this research is to offer strategies for improving legal responses to cybercrime, including strengthening international cooperation, enhancing the technological capacity of law enforcement, and updating regulations. The novelty of this research lies in emphasising the importance of technological adaptation in law enforcement, especially in the face of the increasingly complex and global modus operandi of cybercrime.

Keywords*: Digital Technology; Cybercrime, Law Enforcement; Modus Operandi; regulation*

Abstrak

Penelitian ini bertujuan untuk mengidentifikasi dampak perkembangan teknologi digital terhadap penegakan hukum pidana, terutama dalam konteks kejahatan siber (cybercrime). Penelitian menggunakan metode yuridis normatif dengan pendekatan analisis literatur (library research), yang mencakup kajian terhadap peraturan perundang-undangan, putusan pengadilan, dan studi kasus terkait kejahatan siber. Hasil penelitian menunjukkan bahwa teknologi digital telah memfasilitasi perubahan signifikan dalam modus operandi kejahatan siber, mulai dari phishing hingga serangan menggunakan kecerdasan buatan (AI) dan cryptocurrency, yang mempersulit penegakan hukum. Kontribusi penelitian ini adalah menawarkan strategi peningkatan respons hukum terhadap kejahatan siber, termasuk penguatan kerja sama internasional, peningkatan kapasitas teknologi penegak hukum, serta pembaruan regulasi. Novelti dari penelitian ini terletak pada penekanan pentingnya adaptasi teknologi dalam

penegakan hukum, terutama dalam menghadapi modus operandi kejahatan siber yang semakin kompleks dan global.

Kata Kunci: Teknologi Digital; Cybercrime, Penegakan Hukum; Modus Operandi; Regulasi.

INTRODUCTION

In the digital era, cybercrime is growing along with the rapid advancement of technology. Digital technology has not only changed the way we interact, but it has also opened up new opportunities for criminals. These crimes often cross geographical boundaries, taking advantage of technological loopholes such as encryption and hidden networks (dark web), which make it difficult for traditional law enforcement. This condition requires adaptation from the criminal law system which until now has not been fully able to handle technology-based crime.[1]

One of the main threats in the world of cybercrime is ransomware. Its simple method of dissemination makes it a popular choice among cybercriminals, who often target less vigilant individuals. Dony Koesmandarin, Kaspersky's Territory Manager for Indonesia, explained that perpetrators only need to spread ransomware en masse, hoping that there will be victims who are trapped. In addition to ransomware, other cyber threats include Romance-investment scams, money laundering, illegal gambling, crypto scams, and DDoS attacks.[2] This phenomenon points to the need for further analysis of how digital technologies affect cybercrime as well as the law enforcement system that must continue to evolve to deal with it.[3]

The cybersecurity service provider revealed that the trend of cyberattacks in Indonesia continues to experience a significant increase. During the first semester (H1) of 2024, the number of cyberattacks was recorded to increase up to six times. According to the latest analysis

[1] Amanda Fitria Najwa and Aqila Husna, "Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi," *Jurnal Hukum Dan Sosial Politik* 2, no. 3 (2024): 126–35.

[2] "Tren Kejahatan Siber 2024, Ransomware Masih Jadi Ancaman," Diskominfon Kota Lhokseumawe, 2024, https://kominfo.lhokseumawekota.go.id/berita/read/tren-kejahatan-siber-2024-ransomware-masih-jadi-ancaman-202402281709082917.

[3] Dkk Olukunle, "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System," *World Journal Of Advanced Research and Reviews*, 2024, https://doi.org/doi: 10.30574/wjarr.2024.21.2.0438.

report from AwanPintar.id, the total number of cyberattacks in Indonesia reached 2,499,486,085 throughout the first half of 2024. This number represents a drastic increase compared to the same period the previous year, which recorded 347,172,666 attacks. In other words, Indonesia experiences an average of 13,733,440 attacks per day, or the equivalent of 158 attacks per second.[4]

The main problem is how digital technology changes the modus operandi of cybercrime and how law enforcement can respond effectively. Technology allows perpetrators to evade detection, while law enforcement is still limited in its technological capacity.[5] Existing regulations are often lagging behind, creating a gap between the development of crime and its handling. The urgency of this research lies in the urgent need to update law enforcement strategies to be more responsive to cybercrime, both in terms of prevention and handling of complex cases.

The purpose of this research is to identify the impact of digital technology on the modus operandi of cybercrime and formulate strategies that can improve the response and prevention of this crime. Such strategies may include enhancing the technological capacity of law enforcement, international cooperation, and updating regulations that are more relevant to cybercrime.

The modus operandi is a Latin phrase meaning "way of operating." In the context of criminal law, this term refers to a typical method or pattern used in committing criminal acts. This pattern is so unique that different acts of crime can be identified as the same individual act. The modus operandi is often the basis for receiving evidence related to other related crimes.[6]

This research is expected to contribute to the development of science, especially in the field of criminal law and law enforcement related to cybercrime. In practical terms, the results of this research can be used as a reference for policymakers, law enforcement, and the public

[4] KumparanTech, "Serangan Siber Ke RI Naik 6 Kali Lipat Pada H1 2024, Mayoritas Dari Dalam Negeri," Kumparan.com, 2024.

[5] Abdullah Pakarti, Muhammad Husni, Diana Farid, Hendriana, Usep Saepullah, dan Imam Sucipto. 2023. "Pengaruh Perkembangan Teknologi Terhadap Perlindungan Privasi Dalam Hukum Perdata". SULTAN ADAM : Jurnal Hukum Dan Sosial 1 (2):204-12. https://qjurnal.my.id/index.php/sultanadam/article/view/418.

[6] Definisi Fex, "Modus Operandi," Legal Information Institute, 2020, https://www-law-cornell-edu.translate.goog/wex/modus_operandi?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=wa.

to understand the importance of legal modernization in dealing with technology-based crime. This research also aims to provide alternative solutions that are more effective and can be directly applied in law enforcement practices in the field, by emphasizing the importance of global cooperation and improving the capabilities of law enforcement technology in various countries.

This study seeks to fill the gap in previous studies related to the influence of digital technology on criminal law enforcement, especially in the context of cybercrime. Although there have been several previous studies examining cybercrime, no one has specifically discussed the change in modus operandi due to the development of digital technology and its implications for the criminal law enforcement system in Indonesia.

For example, Irma Yurita, et al. conducted research in the Law Journal, Legalita (2023) with an article entitled "The Influence of Technological Advances on the Development of Cybercrime (study of cases of pising as a threat to digital security)", The results of the study show that technological advances have led to an increase in the complexity and frequency of phishing attacks, making individuals more vulnerable to online fraud. Research by Wahyu Beny Mukti, et al. in the USM Law Review Journal (2020) entitled "Information Technology Regulatory Efforts in Facing Cyber Attacks to Maintain the Sovereignty of the Unitary State of the Republic of Indonesia", the research shows that the ITE Law has not been fully able to regulate broad aspects of cyberspace, so it is necessary to strengthen regulations to protect information technology users. Research conducted by Ahmad Habib Al Faraby in Maraja Jurnal (2024) entitled "ITE Development in Indonesia (A Study of the Role of Police Investigators in Handling Information Misuse and Electronic Transactions)" identifies marriage agreement agreements as included in the category of preventive legal protection. This research emphasizes the importance of strengthening the law and an effective law enforcement system, as well as increasing public awareness about ITE risks. Cross-sector cooperation and targeted education programs are also considered crucial to overcome the challenges of ITE abuse in the future.

This research is urgent because the ever-changing technological developments threaten the effectiveness of law enforcement if not immediately balanced with appropriate adjustments. Without a strong strategy, cybercrime will be increasingly difficult to handle, so this

research aims to offer solutions that can be applied practically in the context of criminal law in the digital era.

RESEARCH METHODS

This research is a normative juridical research that uses a literature analysis approach (*library research*) to explore the influence of digital technology on criminal law enforcement, especially related to cybercrime. This research examines laws and regulations, official documents, court decisions, and relevant academic studies. The subject of this research includes various legal sources such as laws, regulations, international agreements related to cyber law enforcement, and documents from law enforcement agencies related to the handling of cybercrime. In addition, the research also includes cybercrime case studies that are analyzed from court decisions.

The research begins by identifying applicable laws and regulations related to cybercrime, followed by an analysis of changes in the modus operandi of cybercrime due to the development of digital technology. Data was collected through literature review and processed using the content analysis method against regulations, as well as case analysis to understand challenges in criminal law enforcement. The instrument used is a systematic literature review guideline to collect and classify data from various sources. In addition, legal text analysis software is used to map laws and regulations and assess gaps in existing regulations.

The data were analyzed in a qualitative descriptive manner using a normative legal approach. This analysis technique emphasizes the evaluation and interpretation of the content of laws and legal documents related to cybercrime. Primary data from regulations are combined with secondary data from academic studies and case study reports to provide a comprehensive understanding of the impact of digital technologies on law enforcement. As a literature review research, this study does not involve human subjects, so it does not require ethical permission. However, all sources of information are respected and properly cited according to academic standards.

RESULTS AND DISCUSSION

Digital Technology Changes Cybercrime Modus Operandi And Affects Criminal Law Enforcement

In this modern era, digital technology has changed many aspects of our lives, including the way crimes are committed. In the past, crimes were more common physically and limited to a specific location. Now, with the internet, crimes can be committed from anywhere, even from the comfort of the perpetrator's home. This change clearly shows how

sophisticated the world of cybercrime is, where the perpetrators are able to reach victims in distant parts of the world with just a few clicks.[7]

Cybercrime, or cybercrime, utilizes a variety of technological tools to create increasingly diverse and complex crimes. Starting from identity theft to financial fraud, everything can be done easily by the perpetrator. For example, malware and ransomware are now the main weapons for cybercriminals. Malware is used to infiltrate computer systems and steal data, while ransomware threatens to lock the victim's data until the ransom is paid. Phishing techniques are also a common method where perpetrators pretend to be trusted parties to obtain the victim's personal information.[8]

Identity theft cases will experience a sharp spike in 2024. Of the 5.7 million reports received by the FTC, as many as 1.4 million (25%) of them were related to identity theft. The FTC separatates identity theft as a special category that differs from fraud in its report.

A number of job applicants in Cililitan, East Jakarta, fell victim to fraud after their personal data was used to apply for online loans (pinjol) without their knowledge, causing losses of up to Rp 1.1 billion. This fraud mode was carried out by a woman with the initials R, who pretended to be a labor distributor at a cellphone counter. The victim was asked to submit an identity such as an ID card and selfie as a condition for a job application. A total of 26 job applicants were affected, and this case has been reported to the East Jakarta Metro Police for further investigation.[9]

Endang became a victim of online fraud after clicking on a fake invitation sent through a short message application. The invitation was in the form of an APK file disguised as a family invitation, but it turned out to be aimed at stealing personal data and draining account balances. After clicking the invitation, Endang's balance decreases without him making any transactions. Luckily, his quick action to report to Bank BRI and change the security code succeeded in minimizing the loss to only

[7] Marzuki Ismail, "Digital Policing; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian Untuk Mencegah Kejahatan Siber (Cybercrime)," *Jurnal Ilmu Kepolisian* 17, no. 3 (2023): 15.

[8] Ferry Irawan Febriansyah, Alfalachu Indiantoro, and Afiful Ikhwan, "Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional," *Legal Standing: Jurnal Ilmu Hukum* 7, no. 2 (2023): 242–55.

[9] Wildan Noviansah, "Terungkap Modus 'Pencuri' Data Pelamar Kerja Buat Pinjol Hingga Rp 1,1 M," News.detik.com, 2024, https://news.detik.com/berita/d-7429484/terungkap-modus-pencuri-data-pelamar-kerja-buat-pinjol-hingga-rp-1-1-m.

150 thousand rupiah. This case is a warning for the public to be aware of online fraud, especially those that use fake digital invitations.[10]

One major challenge in dealing with cybercrime is its nature, which knows no boundaries. Many of these crimes involve perpetrators and victims who are in different countries, which makes it difficult for law enforcement to coordinate. Differences in legal systems in each country are often an obstacle, so international cooperation is needed to overcome this problem.[11]

Digital technology has drastically changed the modus operandi in cybercrime and affected criminal law enforcement in various parts of the world. One of the main findings of the related study shows that technological advances have made criminals more sophisticated in planning and executing cybercrimes, which has an impact on law enforcement who must pursue these developments. Digital technology facilitates various types of crimes, from *phishing*, *hacking*, to *ransomware*, which threaten the integrity of personal data, financial security, and the country's vital infrastructure.[12]

The modus operandi of cybercrime is also growing with the existence of *artificial intelligence* (AI) and *machine learning*, where criminals can automate cyberattacks on a large scale with little human intervention. This technology is used in more sophisticated and personalized phishing attacks, called *spear-phishing*, where victims are specifically targeted using data collected from social media accounts or publicly available information.[13]

Cryptocurrencies, such as Bitcoin, have added a new layer to cybercrime operations by enabling financial transactions that are difficult to trace. Crypto is often used in ransomware cases, where

[10] Dailypost.id, "Terlanjur Klik Undangan Via WA, Saldo Endang Hilang Secara Misterius," Dailypost.id, 2024, https://dailypost.id/news/terlanjur-klik-undangan-via-wa-saldo-endang-hilang-secara-misterius/.

[11] Ita Musarrofa and Holilur Rohman, "'Urf of Cyberspace: Solutions to the Problems of Islamic Law in the Digital Age," *Al-Ahkam* 33, no. 1 (2023): 63–88, https://doi.org/10.21580/ahkam.2023.33.1.13236.

[12] Wahyu Beny Mukti Setiyawan, Erifendi Churniawan, and Femmy Silaswaty Faried, "Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State Sovereignty of the Republic of Indonesia," *Urnal USM Law* 3, no. 2 (2020): 275–95.

[13] Wahyu Beny Mukti Setiawan, Erifendi Churniawan, and Femmy Silaswaty Faried, "Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber (Cyber Attack) Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia," *Jurnal USM Law Review* 3, no. 2 (2020): 275–95.

victims are forced to pay a ransom in the form of a digital currency that is difficult for authorities to identify. This creates new challenges in tracking and breaking the chain of cybercrime related to ransom or other illegal financial activities.[14]

In addition, *the dark web* has become a means for criminals to conduct illegal transactions anonymously. Trading of personal data, illegal goods, and even cybercrime services such as *hacking-as-a-service* can be found in this *marketplace*. The anonymity provided by *the dark web* adds an extra layer of protection for bad actors, making it difficult for law enforcement to track their activities.[15]

Law enforcement in the face of cybercrime faces many challenges, one of which is the issue *of encryption*. Bad actors often use encryption to protect their communications and data, making them difficult for authorities to access. In addition, the growing development of technologies such as *virtual private networks* (VPNs) allows perpetrators to hide their identities, adding complexity for law enforcement in tracking cybercrime.[16]

Lack of effective international cooperation in law enforcement against cybercrime. Although several countries have cooperated through initiatives such as *the Budapest Convention on Cybercrime*, jurisdictional barriers often make the law enforcement process slow and ineffective. Criminals can easily move their operations from one country to another to avoid prosecution. Anonymity in cyberspace is making things worse. By easily hiding their identity through various means such as VPNs, perpetrators feel safe and more daring to commit crimes. As a result, the investigation process becomes more complicated for law enforcement who are trying to identify and arrest the perpetrators.[17]

However, there is a positive side to this technological advancement. Law enforcement now has more sophisticated digital forensic tools to track the digital footprint of perpetrators, such as log

[14] Kapinus Oksana, "Digitalization of Crime and Criminal Law," 2022, https://doi.org/10.17150/2411-6262.2022.13(1).22.

[15] Uswatun Hasanah, "The Effectiveness Of Islamic Law Implementation To Address Cyber Crime: Studies In Arab, Brunei Darussalam, And China," *Al-Ahkam Jurnal Ilmu Syari'ah Dan Hukum* 3, no. 2 (2018): 107–22, https://doi.org/10.22515/alahkam.v3i2.1348.

[16] Edy Susanto et al., "Manajemen Keamanan Cyber Di Era Digital," *Journal of Business And Entrepreneurship* 11, no. 1 (2023): 23–33.

[17] Yogi Oktafian Arisandy, "Penegakan Hukum Terhadap Cyber Crime Hacker," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 3 (2020): 162–69.

data and IP addresses. By utilizing this technology, they can gather stronger evidence to bring the perpetrator to justice.[18]

However, while technology offers opportunities, there are still legal hurdles to face. Many countries do not have adequate regulations to deal with increasingly complex cybercrime. This legal loophole is often used by perpetrators to avoid punishment. In Indonesia, the Electronic Information and Transaction Law No. 1 of 2024 is the basis for handling cybercrime, in Article 28 paragraph (1) reads as follows:

> "Any Person knowingly distributes and/or transmits Electronic Information and/or Electronic Documents that contain false notices or misleading information that results in material losses to consumers in Electronic Transactions."

Then, people who violate the provisions in Article 28 paragraph (1) of the ITE Bill can be imprisoned for a maximum of 6 years and/or fined a maximum of IDR 1 billion, as stipulated in Article 45A paragraph (1) of the ITE Bill. but many argue that this law still needs to be updated to be more relevant.[19] Some of the issues of concern related to the ITE Law include:

1. Ambiguity of Definitions in the ITE Law
   Articles in the ITE Law, such as Article 27 and Article 28 on the dissemination of false or misleading information, are often interpreted broadly. This raises concerns about freedom of expression as the definition of harmful information has not been clearly defined. Clearer and more specific revisions are needed to avoid multiple interpretations and ensure that implementation is in line with human rights.
2. Regulations That Are Not Responsive to Technological Developments
   The current ITE Law is not able to capture all aspects related to the development of new technology-based crimes, such as cyberattacks involving artificial intelligence (AI) and the use of cryptocurrencies. Law enforcement is still constrained in

[18] Zainuddin Kasim, "Kebijakan Hukum Pidana Untuk Penanggulangan Cyber Crime Di Indonesia," *Indragiri Law Review* 2, no. 1 (2024): 18–24.

[19] Ahmad Habib Al Faraby, "ITE) DI INDONESIA (Suatu Kajian Dari Peran Penyidik Kepolisian Dalam Menangani Penyalahgunaan Informasi Dan Transaksi Elektronika (ITE)," *Faraby Meraja Journal* 7, no. 1 (2024): 48–61.

handling these cases because the law does not regulate in detail how these new crimes are handled.

3. Weak Law Enforcement
   Technologies such as encryption and the dark web complicate the investigation process. Law enforcement is often not equipped with enough tools and skills to deal with these technology-based crimes. An update in the ITE Law should include an obligation to increase the capacity of law enforcement technology.
4. Lack of Data Protection
   The current ITE Law does not provide sufficient protection regarding data breaches. Many cases of data leakage and misuse of personal information have not been properly accommodated by this regulation. The revision of the ITE Law needs to tighten sanctions against companies that are negligent in safeguarding customer data and set strict security standards.
5. The Need for International Harmonization
   The ITE Law also does not accommodate cross-border cooperation in dealing with cybercrime. Given the large number of cybercrimes committed by foreign perpetrators, it is necessary to strengthen regulations to encourage international collaboration in cyber law enforcement.

Through this juridical analysis, it can be concluded that the ITE Law requires updates to adjust to technological changes and rapidly evolving social dynamics. Such updates should include strengthening definitions, increasing the technological capacity of law enforcement, stronger data protection, and regulations that are more responsive to new crimes arising from digital technology.

Data breaches are a significant security threat, where hackers enter data networks to gain access to confidential and sensitive personal information for financial gain. Losses resulting from cybercrime are estimated to reach $9.5 trillion by 2024, slightly lower than the previous projection of $10.5 trillion for 2025 (Embroker, Govtech).[20] This demonstrates the ongoing and significant financial impact of cyber

[20] Naida, "Mind-Blowing Cybersecurity Statistics in 2024," *Softactivity-Com.Translate.Goog*, 2024, https://www-softactivity-com.translate.goog/ideas/cybersecurity-statistics/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc.

threats on companies. Where there are 26 residents in East Jakarta who are victims of the misuse of ID card data for online loans.[21]

The protection of privacy and personal data is becoming an increasingly important issue. In many cases, victims' personal data is stolen and misused, leading to financial and psychological losses for them. Therefore, it is important to have a strong data protection policy so that people feel safe when doing activities in cyberspace. The speed of technological change is also a challenge. Cybercrime continues to evolve as technology advances, and law enforcement can often only react after a crime has occurred. Therefore, it is important to have a more proactive approach to preventing cybercrime before it happens.[22]

One noteworthy development is the emergence of the Internet of Things (IoT). Many devices are now connected to the internet, from security cameras to cars. However, it also opens up opportunities for cybercriminals to exploit vulnerabilities in these devices, making it easier for them to attack.[23]

Strategies That Can Be Implemented To Improve Response And Prevention Against Cybercrime

In the midst of increasingly rapid technological developments, cybercrime has become a real threat faced by many countries around the world. Technology, which is supposed to make our lives easier, now also provides opportunities for criminals to carry out attacks, such as data theft, hacking, and the spread of malware. This problem not only impacts individuals, but also companies and even the critical infrastructure of a country. Effective law enforcement against cybercrime is now a very urgent task for the government and law enforcement officials.[24]

Dealing with cybercrime clearly cannot use conventional approaches. This type of crime crosses geographical boundaries and often occurs in cyberspace, requiring smarter and more complex

[21] Aguido Aidro, "26 Warga Jadi Korban Pencurian Data Pribadi Untuk Pinjol," Kompas.id, 2024, https://www.kompas.id/baca/metro/2024/07/08/26-jadi-korban-pencurian-data-pribadi-untuk-pinjol.

[22] Ria Ermina Purba et al., "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital," *Mandub: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2, no. 2 (2024): 167–76.

[23] Adji Saputra, Kristiawanto Kristiawanto, and Mohamad Ismed, "Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia," *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (2024): 63–70.

[24] Zulhamid Ridho et al., "Implementasi Program PELITA: Sosialisasi Dan Pencegahan Cyber Bullying Melalui Literasi," *Jurnal Pengabdian Masyarakat Bangsa* 2, no. 7 (2024): 2549–61.

handling. Law enforcers must understand the ever-evolving technology, and be able to follow the mindset of cybercriminals who are highly adaptive. Without the right strategy, law enforcement efforts can be slow and ineffective in dealing with threats that move so quickly. For this reason, a strategy that is not only reactive but also preventive is needed.[25]

The strategy for improving response and prevention to cybercrime is, ***First***, to overcome the increasingly sophisticated threat of cybercrime, law enforcement officials must have access to cutting-edge technology. Technologies such as digital forensic analysis software allow investigators to extract and analyze digital evidence from devices used in crimes. By using this tool, the authorities can find the digital traces of the perpetrators more quickly and accurately. In addition, the integration of artificial intelligence (AI) in the investigation process can make it easier to detect complex crime patterns and accelerate the analysis of big data.[26]

In addition to digital forensics technology, it is important for law enforcement officials to be equipped with powerful cybersecurity tools. For example, malware tracking software can help identify the source of cyberattacks and map the criminal networks involved. Advanced encryption technology is also necessary to protect sensitive information during investigations. With this kind of technology, data collected and stored by law enforcement can be kept safe from hacking or manipulation by unauthorized third parties.

Law enforcement officials also need to invest in the development of real-time cyber activity monitoring devices. This monitoring allows for early detection of suspicious activity that indicates a cyberattack. With the ability to continuously monitor data traffic on the network, law enforcement officials can immediately respond to threats before data damage or theft occurs. This will also help them to be more proactive in dealing with cybercrime threats, rather than just being reactive after the incident has taken place.[27]

---

[25] Soecipto Soecipto, "Optimalisasi Hukum Siber (Cyber Law) Dalam Penanggulangan Kejahatan Penipuan Melalui Internet Dalam Menyelamatkan Kehidupan Masyarakat.," *TEKNOLOGI NUSANTARA* 4, no. 2 (2022).

[26] Lutfi Aziz Febrika Ardy et al., "Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial," *Journal of Internet and Software Engineering* 1, no. 4 (2024): 11.

[27] Tri Ginanjar Laksana and Sri Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisiplin* 3, no. 01 (2024): 109–22.

Second, law enforcement officials need to take part in ongoing training on the latest developments in cybercrime. This training should include effective investigative techniques for technology-based crimes. They need to be equipped with the skills to understand the encryption methods used by criminals and how to crack them without damaging digital evidence. Comprehensive education will make the apparatus better prepared to deal with the challenges faced in law enforcement against cybercrime.[28]

In addition, training should include case studies from various countries on successes and failures in handling cybercrime. This will help law enforcement officials learn from practical experience, understand how cybercrime cases can occur, and what preventive measures can be applied. Presenting international cybersecurity experts in the training can also enrich the perspective of the authorities in dealing with this cross-border crime.

Training must be carried out regularly so that the apparatus always keeps up with the latest developments in the world of information technology and cyber threats. With the rapid development of technology, cybercrime methods are also constantly changing. If the authorities are not equipped with the latest knowledge, they will find it difficult to keep up with the speed of the perpetrators. Therefore, regularly scheduled training is essential to maintain the quality of response to cybercrime.[29]

Third, cross-border cybercrime makes international cooperation a key element in its prevention efforts. Countries need to forge strong partnerships to share information on emerging threats. Real-time exchange of information can help other countries to prepare for similar potential attacks. Without this cooperation, law enforcement in one country will be hampered if the perpetrators are in different jurisdictions, making the process of arrest difficult.[30]

International cooperation should also include harmonization of regulations between countries. With uniform regulations, criminals

---

[28] Edy Soesanto et al., "Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File," *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen* 1, no. 2 (2023): 172–91.

[29] Dewi Rizka Yuniarti et al., "Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem Logistik Di Era Digital," *Jurnal Bisnis, Logistik Dan Supply Chain (Blogchain)* 3, no. 1 (2023): 23–32.

[30] Maluleke Mandlenkosi, Richard, Mphatheni., Witness, "Cybersecurity as a Response to Combating Cybercrime," *International Journal of Research In Business and Social Science*, 2022, https://doi.org/doi: 10.20525/ijrbs.v11i4.1714.

cannot seek "refuge" in countries where regulations are more lax. This is important to create a more conducive environment for effective law enforcement against cybercrime. For example, through international agreements, countries can agree on minimum standards in data protection as well as severe sanctions for violations related to cybercrime.

In addition, international cooperation also involves technical assistance, such as training for law enforcement officials in developing countries that do not yet have adequate infrastructure and technology. Developed countries that have more advanced digital forensic technology can provide training and share resources with other countries. Thus, the handling of cybercrime can be more equitable and efficient around the world, not only concentrated in countries with high-tech capacity.[31]

Fourth, public awareness about the risk of cybercrime needs to be increased through intensive public campaigns. People are often easy targets for cybercriminals due to a lack of knowledge about how to protect themselves in the digital world. Through awareness campaigns, individuals can be provided with information on the importance of keeping personal data confidential, recognizing phishing, and how to avoid malware. These educational programs can be carried out through various media, including television, the internet, and seminars in schools.[32]

In addition to campaigns, governments and non-governmental organizations can work together to provide online educational materials that are easily accessible to the general public. Cybersecurity education is not only important for individuals, but also for small and medium-sized enterprises that are often the target of attacks. Through free webinars or training modules, people can learn basic ways to protect their information systems from cyber threats.

High public awareness of the risk of cybercrime will help reduce the number of victims who are deceived by technology-based crimes. Individuals who understand this threat are more vigilant and tend to take preventive measures. For example, they will be more selective in sharing

[31] Dkk Edwin, "Investigating the Intersection of Cybercrime and Machine Learning: Strategies for Prevention and Detection," 2023, https://doi.org/doi: 10.1109/ICIDCA56705.2023.10099631.

[32] Supanto Supanto et al., "Pencegahan Dan Penanggulangan Kejahatan Teknologi Informasi Di Wilayah Pdm Kabupaten Klaten Melalui Metode Sosialisasi Interaktif," *Gema Keadilan* 10, no. 3 (2023): 170–82.

personal information on social media or more cautious when downloading apps from unknown sources. This is an effective form of prevention from the end user side who is the main target of cybercriminals.[33]

Fifth, regulations governing the protection of personal data must continue to be developed in line with the increasing threat of cybercrime. This policy should include clear and firm sanctions for companies or individuals who are negligent in protecting the data they manage. With strict sanctions, companies will be more encouraged to comply with the rules and implement adequate security measures to protect user data. This regulation also needs to cover the company's responsibility in the event of a data leak.[34]

In addition to data protection regulations, there are also minimum security standards that must be met by companies that manage personal data. These standards should include the use of encryption, periodic security audits, as well as early detection systems against hacking attempts. Strict security standards will ensure that people's personal data is properly safeguarded, and companies that fail to meet these standards should be held legally responsible for any data leaks that occur.

Supervision of the implementation of data protection policies must be strictly carried out by the relevant authorities. It is not enough to have good regulations, but implementation in the field must also be well supervised. The authority that oversees data protection must have the authority to conduct inspections and impose sanctions if violations are found. Thus, existing regulations can run effectively and provide maximum protection for people's personal data.[35]

Sixth, Artificial Intelligence (AI) can be integrated in security systems to detect anomalies that have the potential to become cyber threats. AI systems are able to process large amounts of data quickly and accurately, so they can identify suspicious patterns that may not be visible to humans. For example, AI can detect distributed denial of

[33] Ihsania Karin Azzani, Susilo Adi Purwantoro, and Hikmat Zakky Almubaroq, "Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja Paruh Waktu Sebagai Ancaman Negara," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 10, no. 7 (2023): 3556–68.

[34] Muhammad Farhan et al., "Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber," *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora* 1, no. 6 (2023): 8–20.

[35] Balqis Tsabitah Azzahrah et al., "Tantangan Pertahanan Dan Keamanan Data Cyber Dalam Era Digital: Studi Kasus Dan Implementasi," *Jurnal Pendidikan Tambusai* 8, no. 2 (2024): 23934–43.

service (DDoS) attacks before their impact is widespread, so mitigation actions can be taken immediately. The use of AI in security systems provides advantages in terms of speed of response to attacks.[36]

In addition, AI can be used to analyze user behavior online, and alert law enforcement when such behavior deviates from the norm. With this technology, criminal attempts such as identity theft or fraud can be anticipated before harm is done. AI can also help in the digital forensics process, where complex algorithms can be used to analyze the digital footprint of cybercrime offenders. This makes investigations faster and more efficient.

In preventing cybercrime, AI can also be applied to filter potentially unlawful content on the internet. This technology allows the system to automatically block access to content that is considered malicious, such as phishing websites or malware. Thus, potential losses for users can be minimized. However, the use of AI in law enforcement and cybersecurity must be balanced with strict regulations so as not to violate individual privacy or be used arbitrarily.[37]

CONCLUSION

The results of the study concluded that digital technology has drastically changed the modus operandi of cybercrime, with advanced tools such as AI, IoT, malware, and ransomware. Law enforcement faces major challenges, especially in dealing with cross-border crime powered by cryptocurrencies and the dark web. Differences in jurisdiction as well as encryption technology complicate the investigation. For this reason, law enforcement needs to increase technological capacity and encourage stronger international cooperation. Further research is suggested to focus on the use of AI and IoT in cybercrime as well as more effective prevention strategies. In addition, regulatory updates relevant to technological developments are urgently needed, as well as increased public awareness of personal data security to prevent further cybercrime.

[36] Yusep Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, no. 02 (2022): 295–316.

[37] Aisyah Putri Nabila, Nathania Aurell Manabung, and Aquilla Cinta Ramadhansha, "Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional," *Indonesian Journal of Law* 1, no. 1 (2024): 26–37.

BIBLIOGRAPHY

Aidro, Aguido. "26 Warga Jadi Korban Pencurian Data Pribadi Untuk Pinjol." Kompas.id, 2024. https://www.kompas.id/baca/metro/2024/07/08/26-jadi-korban-pencurian-data-pribadi-untuk-pinjol.

Ardy, Lutfi Aziz Febrika, Iklima Istiqomah, Angga Eben Ezer, and Shelvie Nidya Neyman. "Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial." *Journal of Internet and Software Engineering* 1, no. 4 (2024): 11.

Abdullah Pakarti, Muhammad Husni, Diana Farid, Hendriana, Usep Saepullah, dan Imam Sucipto. 2023. "Pengaruh Perkembangan Teknologi Terhadap Perlindungan Privasi Dalam Hukum Perdata". Sultan Adam: Jurnal Hukum Dan Sosial 1 (2):204-12. https://qjurnal.my.id/index.php/sultanadam/article/view/418.

Arisandy, Yogi Oktafian. "Penegakan Hukum Terhadap Cyber Crime Hacker." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 3 (2020): 162–69.

Azzahrah, Balqis Tsabitah, Muhammad Naufal Razzan Hamdi, Rasheesa Ryash Raynee, Zulfa Layla Ni'matussa'idah, and Subakdi Subakdi. "Tantangan Pertahanan Dan Keamanan Data Cyber Dalam Era Digital: Studi Kasus Dan Implementasi." *Jurnal Pendidikan Tambusai* 8, no. 2 (2024): 23934–43.

Azzani, Ihsania Karin, Susilo Adi Purwantoro, and Hikmat Zakky Almubaroq. "Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja Paruh Waktu Sebagai Ancaman Negara." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 10, no. 7 (2023): 3556–68.

Dailypost.id. "Terlanjur Klik Undangan Via WA, Saldo Endang Hilang Secara Misterius." Dailypost.id, 2024. https://dailypost.id/news/terlanjur-klik-undangan-via-wa-saldo-endang-hilang-secara-misterius/.

Edwin, Dkk. "Investigating the Intersection of Cybercrime and Machine Learning: Strategies for Prevention and Detection," 2023. https://doi.org/doi: 10.1109/ICIDCA56705.2023.10099631.

Faraby, Ahmad Habib Al. "ITE) DI INDONESIA (Suatu Kajian Dari Peran Penyidik Kepolisian Dalam Menangani Penyalahgunaan Informasi Dan Transaksi Elektronika (ITE)." *Faraby Meraja Journal* 7, no. 1 (2024): 48–61.

Farhan, Muhammad, Rajasa Syaefunaldi, Dhifa Ridho Dwiputra

Hidayat, and Asmak Ul Hosnah. "Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber." *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora* 1, no. 6 (2023): 8–20.

Febriansyah, Ferry Irawan, Alfalachu Indiantoro, and Afiful Ikhwan. "Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional." *Legal Standing: Jurnal Ilmu Hukum* 7, no. 2 (2023): 242–55.

Fex, Definisi. "Modus Operandi." Legal Information Institute, 2020. https://www-law-cornell-edu.translate.goog/wex/modus_operandi?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=wa.

Ginanjar, Yusep. "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara." *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, no. 02 (2022): 295–316.

Hasanah, Uswatun. "The Effectiveness Of Islamic Law Implementation To Address Cyber Crime: Studies In Arab, Brunei Darussalam, And China." *Al-Ahkam Jurnal Ilmu Syari'ah Dan Hukum* 3, no. 2 (2018): 107–22. https://doi.org/10.22515/alahkam.v3i2.1348.

Ismail, Marzuki. "Digital Policing; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian Untuk Mencegah Kejahatan Siber (Cybercrime)." *Jurnal Ilmu Kepolisian* 17, no. 3 (2023): 15.

Kasim, Zainuddin. "Kebijakan Hukum Pidana Untuk Penanggulangan Cyber Crime Di Indonesia." *Indragiri Law Review* 2, no. 1 (2024): 18–24.

KumparanTech. "Serangan Siber Ke RI Naik 6 Kali Lipat Pada H1 2024, Mayoritas Dari Dalam Negeri." Kumparan.com, 2024.

Laksana, Tri Ginanjar, and Sri Mulyani. "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan." *Jurnal Ilmiah Multidisiplin* 3, no. 01 (2024): 109–22.

Mandlenkosi, Richard, Mphatheni., Witness, Maluleke. "Cybersecurity as a Response to Combating Cybercrime." *International Journal of Research In Business and Social Science*, 2022. https://doi.org/doi: 10.20525/ijrbs.v11i4.1714.

Musarrofa, Ita, and Holilur Rohman. "'Urf of Cyberspace: Solutions to the Problems of Islamic Law in the Digital Age." *Al-Ahkam* 33, no. 1 (2023): 63–88.

https://doi.org/10.21580/ahkam.2023.33.1.13236.

Nabila, Aisyah Putri, Nathania Aurell Manabung, and Aquilla Cinta Ramadhansha. "Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional." *Indonesian Journal of Law* 1, no. 1 (2024): 26–37.

Naida. "Mind-Blowing Cybersecurity Statistics in 2024." *Softactivity-Com.Translate.Goog*, 2024. https://www-softactivity-com.translate.goog/ideas/cybersecurity-statistics/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc.

Najwa, Amanda Fitria, and Aqila Husna. "Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi." *Jurnal Hukum Dan Sosial Politik* 2, no. 3 (2024): 126–35.

Noviansah, Wildan. "Terungkap Modus 'Pencuri' Data Pelamar Kerja Buat Pinjol Hingga Rp 1,1 M." News.detik.com, 2024. https://news.detik.com/berita/d-7429484/terungkap-modus-pencuri-data-pelamar-kerja-buat-pinjol-hingga-rp-1-1-m.

Oksana, Kapinus. "Digitalization of Crime and Criminal Law," 2022. https://doi.org/10.17150/2411-6262.2022.13(1).22.

Olukunle, Dkk. "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System." *World Journal Of Advanced Research and Reviews*, 2024. https://doi.org/doi: 10.30574/wjarr.2024.21.2.0438.

Purba, Ria Ermina, Dewi Maharani, M Akbar Adjiguna BMY, and Raudatul Zahra Al Zahra. "Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital." *Mandub: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2, no. 2 (2024): 167–76.

Ridho, Zulhamid, Oktiva Ramadani, Muhammad Ikhsan, Syakira Syafia A'izza, Arvitori Amenda, Salsabilla Ar Razzaq Syukra, Dini Allifa, Alvin Afrinaldo, Saifana Kalda, and Shabrina Bella Puspita. "Implementasi Program PELITA: Sosialisasi Dan Pencegahan Cyber Bullying Melalui Literasi." *Jurnal Pengabdian Masyarakat Bangsa* 2, no. 7 (2024): 2549–61.

Saputra, Adji, Kristiawanto Kristiawanto, and Mohamad Ismed. "Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia." *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (2024): 63–70.

Setiawan, Wahyu Beny Mukti, Erifendi Churniawan, and Femmy Silaswaty Faried. "Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber (Cyber Attack) Guna Menjaga

Kedaulatan Negara Kesatuan Republik Indonesia." *Jurnal USM Law Review* 3, no. 2 (2020): 275–95.

Setiyawan, Wahyu Beny Mukti, Erifendi Churniawan, and Femmy Silaswaty Faried. "Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State Sovereignty of the Republic of Indonesia." *Urnal USM Law* 3, no. 2 (2020): 275–95.

Soecipto, Soecipto. "Optimalisasi Hukum Siber (Cyber Law) Dalam Penanggulangan Kejahatan Penipuan Melalui Internet Dalam Menyelamatkan Kehidupan Masyarakat." *TEKNOLOGI NUSANTARA* 4, no. 2 (2022).

Soesanto, Edy, Achmad Romadhon, Bima Dwi Mardika, and Moch Fahmi Setiawan. "Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File." *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen* 1, no. 2 (2023): 172–91.

Supanto, Supanto, Ismunarno Ismunarno, Tika Andarasni Parwitasari, Winarno Budyatmojo, Riska Andi Fitriono, and Siwi Widiyanti. "Pencegahan Dan Penanggulangan Kejahatan Teknologi Informasi Di Wilayah Pdm Kabupaten Klaten Melalui Metode Sosialisasi Interaktif." *Gema Keadilan* 10, no. 3 (2023): 170–82.

Susanto, Edy, Lady Antira, Kevin Kevin, Edo Stanzah, and Assyeh Annasrul Majid. "Manajemen Keamanan Cyber Di Era Digital." *Journal of Business And Entrepreneurship* 11, no. 1 (2023): 23–33.

"Tren Kejahatan Siber 2024, Ransomware Masih Jadi Ancaman." Diskominfon Kota Lhokseumawe, 2024. https://kominfo.lhokseumawekota.go.id/berita/read/tren-kejahatan-siber-2024-ransomware-masih-jadi-ancaman-20240228170908291 7.

Yuniarti, Dewi Rizka, Hafidz Fauzan Alfarizy, Zifron Siallagan, and Mochamad Whilky Rizkyanfi. "Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem Logistik Di Era Digital." *Jurnal Bisnis, Logistik Dan Supply Chain (Blogchain)* 3, no. 1 (2023): 23–32.