International Journal of Contemporary Sciences (IJCS)
Vol. 3, No. 7, 2025: 109-122

Transnational Cyber Crime: Challenges of International Cooperation in Combating Cybercrime

Arum Widiastuti[1*], Yasmirah Mandasari Saragih[2]
[1]Universitas Wahid Hasyim Semarang, [2]Universitas 17 Agustus 1945 Jakarta
Corresponding Author: Arum Widiastuti arumbsb@unwahas.ac.id

A R T I C L E I N F O

Keywords: Transnational Cyber Crime, Cybercrime, International Cooperation, International Law, Cyber Crime Eradication

Received : 5 June
Revised : 20 June
Accepted: 29 July

A B S T R A C T

This study aims to examine the forms of transnational cybercrime, the challenges faced in addressing it, and the importance of international cooperation in efforts to eradicate it. This research uses a qualitative-descriptive method with a normative legal approach, analyzing national legislation and international legal instruments related to cybercrime. The study results show that combating transnational cybercrime faces various challenges, such as differences in legal systems between countries, a lack of extradition mechanisms and mutual legal assistance (MLA), limited law enforcement capacity in developing countries, and technological gaps. Furthermore, there is still no global agreement on the definition and categories of cybercrime. International cooperation is a key factor in combating this crime through the enhanced role of international organizations such as INTERPOL and UNODC, strengthening multilateral legal frameworks like the Budapest Convention, and building technical capacity and information exchange between countries. There is a need for closer global synergy, regulatory harmonization, and political commitment from countries around the world to collectively address cybercrime

INTRODUCTION

The rapid development of information technology has facilitated communication and access to information across countries. However, this progress has also been accompanied by an increase in transnational cybercrime. The characteristic of the cyber world, which is without borders, allows cybercriminals to operate across jurisdictions, making law enforcement more difficult. International cooperation becomes very important in combating cybercrime, but in practice, it faces various challenges, ranging from differences in national laws, political interests, to the limited capacity of law enforcement institutions in certain countries (Kasturirangan & Shankar, 2017).

The challenges of international cooperation in combating cybercrime are very complex and diverse. Some of the main challenges include differences in regulations between countries, limitations in resources and infrastructure, as well as difficulties in cross-border law enforcement. Additionally, the capacity gap between developed and developing countries, a lack of understanding about cybercrime, and insufficient reporting also pose obstacles (Hapsari & Pambayun, 2023).

One way to understand the nature of cybercrime is through network forensics, which is a method for capturing, storing, and analyzing user network data to find the source of system security breaches or issues in information system security. When we talk about this aspect, it certainly involves the OSI layers, which explain how computers can communicate. This does not only involve LAN network systems, but can also encompass larger network systems (Saragih, 2017).

1. Some challenges in efforts to combat cybercrime internationally are (Fahlevy, et al, 2025): 1. Differences in Regulation and Laws: Countries have different laws and regulations related to cybercrime, making it difficult to handle cases involving perpetrators from various jurisdictions.
2. Capacity Gaps: Developing countries often lack adequate resources, technology, and experts to effectively address cybercrime.
3. Cross-Border Law Enforcement Challenges: Law enforcement in cybercrime cases involving perpetrators in different countries is often hindered by differing procedures, lack of extradition agreements, and difficulties in information exchange.
4. Lack of Understanding and Awareness: A lack of understanding about cybercrime, both among the public and law enforcement officials, can hinder prevention and response efforts.
5. Limitations of Cooperation Mechanisms: Existing international cooperation mechanisms may not be sufficient to address all types of cybercrime, especially those involving new and complex technologies.
6. Lack of Reporting: Many victims of cybercrime are reluctant to report incidents for various reasons, including fear of repercussions or lack of trust in law enforcement.

The rapid development of digital technology has brought significant changes to the global order, facilitating economic growth, innovation, and connectivity. However, this transformation has also led to a surge in cybercrime,

posing major challenges for national and international security. According to Andi Hamzah (1989), cybercrime can generally be defined as illegal use of computers (Rai, 2022).

Starting from financial fraud and identity theft to cyber terrorism and data breaches, these challenges are becoming more sophisticated and transnational, necessitating a strong and cooperative regulatory framework. The United Nations Convention against Cybercrime is a global effort to address these challenges. Adopted to encourage international cooperation in combating cybercrime, this convention aims to align legal standards, enhance law enforcement collaboration, and promote capacity building in member countries (Balboni and Pelino, 2013).

LITERATURE REVIEW

According to the United Nations Office on Drugs and Crime (UNODC), transnational cybercrime is a crime committed through computer networks, where the perpetrator, victim, or impact is located in more than one country (UNODC, 2013). Cybercrime includes malware attacks, identity theft, hacking systems, and financial crimes that cause significant losses to individuals, companies, and countries.

Transnational cybercrime is defined as criminal acts committed through or using information and communication technology, which have cross-border dimensions in terms of perpetrators, victims, and the impacts caused. According to international legal literature, transnational cybercrime includes various forms of criminal activities such as online fraud, identity theft, attacks on critical infrastructure, and illegal trade on the darknet (Bunga, 2019).

The Convention on Cybercrime 2001, known as the Budapest Convention, is the first comprehensive international legal instrument addressing issues of cybercrime. This convention includes the harmonization of national laws, enhancement of investigative capacities, and facilitation of international cooperation. However, the adoption and implementation of this convention still face various challenges, particularly related to differences in legal systems and state sovereignty (Bunga, 2020).

One of the fundamental challenges in tackling transnational cybercrime is the issue of jurisdiction. Traditional international law principles based on territoriality struggle to address crimes that occur in cyberspace, which does not recognize geographical boundaries. This creates legal loopholes that can be exploited by cybercriminals.

The legal basis related to transnational cybercrime refers to various international and national regulations governing crimes involving information and communication technology that cross national borders. Some important legal bases related to this issue are (Hui, 2017):

1) The Budapest Convention (Budapest Convention on Cybercrime, 2001) This convention is the first international instrument that regulates cybercrime at a global level. The Budapest Convention addresses computer crimes, such as illegal access to computer systems, the spread of viruses, identity theft, as well as crimes that use technology to carry out criminal actions. Countries

that sign this convention commit to adopting laws and policies that support the eradication of cybercrime.

2) National Regulations (Example: Electronic Information and Transactions Law in Indonesia) In Indonesia, the Electronic Information and Transactions Law (Law No. 11 of 2008 amended by Law No. 19 of 2016) serves as the legal basis for addressing crimes committed through information technology, such as defamation, fraud, and the dissemination of illegal content on the internet. This law grants law enforcement authorities the power to handle domestic cybercrime cases.
3) UN Convention Against Transnational Organized Crime (Palermo Convention, 2000) Although it does not specifically address cybercrime, this convention regulates transnational organized crime, which may include cybercrime involving international networks. Countries that sign this convention are obliged to enhance cooperation in combating cross-border crime, including internet-based crimes.
4) International Cooperation Besides formal regulations, many countries also build bilateral and multilateral cooperation to address transnational cybercrime. For instance, INTERPOL and EUROPOL have special units for dealing with cybercrime involving multiple countries.
5) UNODC (United Nations Office on Drugs and Crime) UNODC plays a role in providing technical assistance and developing countries' capacities to tackle transnational cybercrime through international projects and training.

On the positive side, e-business through the internet has opened a new world of communication for consumers in all aspects of life, but on the negative side, e-business has also created an environment as an open playing field for criminal activities to operate smoothly on a global scale. The introduction and use of electronic money, virtual banks, foreign exchange markets, and online stores have become one of the main factors in the development of new types of transnational cybercrimes. Crimes can be committed thousands of miles away from the actual crime location (Moise, 2014).

In other words, a cybercriminal does not need to leave their own home or crossnational borders to commit acts in several countries around the world. Communication can be routed in various ways, ranging from local telephone companies, long-distance operators, internet service providers, wireless and satellite networks, and may involve computers located in multiple countries before attacking target systems globally. Evidence of cybercrime may even be stored on computers in other countries where the perpetrator carried out their actions (Moitra, 2005).

Countries need to cooperate because cybercriminals are not limited by national or geographical borders, and digital evidence related to one crime can be spread across various regions. While it is essential for countries to have cybercrime laws, the legal authority to assist foreign nations in investigations is equally important, even if the country itself has not suffered any damage and is merely a location for the intruder or a transit site (Ginanjar, 2022).

The idea behind creating international guidelines to combat cybercrime is to facilitate an easy process for conducting digital investigations involving

computers from more than one country, as well as to eliminate areas in the world where cybercriminals are beyond the reach of national law (Sieber, 1998).

However, there are many challenges in international cooperation to combat transnational cybercrime. Harmonizing the criminal laws of a country, the level of such crimes, finding and identifying cross-border perpetrators, securing electronic evidence of their crimes for prosecution, and various other complex jurisdictional issues and procedures arise at every step. This paper discusses approaches to address these difficulties and other challenges faced by law enforcement on the international front (Aini & Lubis, 2024).

METHODOLOGY

The type of research that the author uses in compiling this legal writing is normative juristic research or library research, which is legal research conducted by examining library materials or secondary data consisting of primary legal materials, secondary legal materials, and tertiary legal materials. These materials are systematically organized, reviewed, and then a conclusion is drawn in relation to the problem being researched.

Legal research conducted solely by examining library materials or secondary data can be termed normative legal research or library legal research. By using this type of normative juristic research, the research approach adopted is the legislative approach, which is a research method that involves reviewing laws and regulations related to the legal issues being studied.

The Case Approach is a research approach that is conducted by examining cases related to legal issues that have been encountered and have received decisions that have permanent legal force (inkracht). Legal materials in this research are obtained through literature study, with the technique of searching for legal materials in the form of literature or books being done by making a list of books to be searched, followed by the author searching through books at the Wijaya Kusuma University Library and the Mojokerto City Library. Legal materials in the form of laws, decisions, and scientific articles are obtained from websites related to the Reform of Positive Criminal Law.

RESULTS AND DISCUSSION

A. The Main Challenges in International Cooperation in Combating Cybercrime

1. Jurisdictional Complexity

There are many challenges faced by law enforcement agencies. In this section, the author analyzes the most important ones, such as the lack of harmonization of national criminal laws regarding cybercrime and the difficulty in finding a clear and comprehensive definition of computer-related crimes. With the increasing violations of cybercrime, it is important to highlight issues related to the minimal risk of detection and apprehension. These include the lack of training for investigative officers, unknown or anonymous victims, victims' reluctance to report after encountering cybercrime, difficulties in locating and identifying cross-border perpetrators, and other procedural problems related to such crimes.

The lack of national legal harmonization creates too many difficulties. Without a shared understanding of this issue, countries do not know how to respond. For instance, it is difficult to find an agreement on the general concepts of cybercrime, computer crime, or high technology crime. There has been much debate among experts regarding what is meant by computer crime. However, the different intentions of the authors to be more precise in terms of the scope and use of certain definitions mean that the use of these definitions outside the intended context often leads to inaccuracies, so a universally accepted definition of computer crime has not yet been achieved to this day.

Computer crime can involve traditional criminal activities, all of which generally can be subject to criminal penalties. However, computers and the Internet have created a number of new potential abuses or misuses that can also be deemed criminal. Regarding traditional forms of crime committed through the use of new technology, this update can be made by clarifying or eliminating provisions that are no longer fully adequate, such as laws that cannot create new provisions for new crimes, or unauthorized access to computers or data networks. Thus, any criminal activity conducted exclusively via the internet should be more specifically designated as cybercrime. The term high-tech crime or computer-related crime encompasses both concepts: computer crime and cybercrime.

The digital revolution has transformed the landscape of conventional crime into complex and cross-border cybercrime. Cybercrime has now become a serious threat to national security, economic stability, and the social life of the global community. According to research published in an accredited journal, advancements in digital technology have significantly increased the threats of cybercrime, leading to issues such as identity theft, job loss, and disruptions to critical infrastructure.

The complexity of cybercrime lies in its nature that knows no geographical boundaries, where perpetrators may be in one country while victims and impacts are spread across various countries. This creates unique challenges in law enforcement that require effective international cooperation. Cybercriminals continuously develop new techniques and strategies in carrying out their crimes, hence international responses must be adaptive and coordinated.

One of the fundamental challenges in combating cybercrime is the complexity of jurisdiction. According to international law, countries have certain boundaries in applying jurisdiction for cases involving the interests of other countries. Cross-border cybercrime creates a jurisdictional dilemma in which it is difficult to determine which country has the authority to judge the perpetrators (Bego, et al., 2025). The jurisdictional issue becomes even more complex when the perpetrator, victim, server, and the impact of the crime are spread across various countries. Each country has a different legal system, which can lead to legal conflicts and hinder law enforcement processes.

Cybercrime or cyber criminality is defined as criminal acts that use computers and networks as tools, targets, or places of crime. According to peer-reviewed accredited journals, cybercrime includes various forms of crime ranging from identity theft, denial of service attacks, computer virus releases, to

more complex crimes such as cyberterrorism. The main characteristics of cybercrime that distinguish it from conventional crime are its transnational nature, the use of high technology, and the potential to cause massive losses in a short period of time. Cybercriminals can operate from anywhere in the world and target victims in different countries simultaneously (Djanggih & Qamar, 2018).

International cooperation in combating cybercrime has become an urgent necessity given the cross-border nature of crime. Research shows that the development of cybersecurity and international cooperation in cybersecurity undertaken by Indonesia with other countries has been strengthened by the establishment of the National Cyber and Crypto Agency (BSSN). International cooperation can be categorized as cooperative security based on shared goals, which can be conducted bilaterally or multilaterally. Indonesia's cyber diplomacy has resulted in cooperation with other countries to strengthen cybersecurity as part of national security.

The Budapest Convention is the first international treaty to explicitly focus on cybercrime. This convention aims to serve as an international framework for the harmonization of legislation related to cybercrime and to facilitate the eradication of crimes that use computer networks. The Budapest Convention is regarded as the most comprehensive and coherent international agreement on cybercrime and electronic evidence to date. This convention is more than just a legal document; it is a framework that allows hundreds of practitioners from member countries to share experiences and create connections that facilitate cooperation in specific cases (Farhan et al., 2023).

2. *The extent of cybercrime*

Although it is possible to provide an accurate description of various types of computer violations committed, it is difficult to give an accurate picture of the level of losses and the actual number of cybercrimes. Crime statistics do not represent the actual number of violations. The number of hidden crimes that are unreported or unknown can be attributed to the following reasons (Ginanjar, 2022):

a. High-level information and communication technology. One of the reasons why cybercrime is very difficult to detect is due to the very large storage capacity of computers, the ability to manipulate, and the speed at which computers and networks operate. Unlike most types of conventional crime, victims are informed about the incident long after the crime occurs.
b. Lack of training for investigative officers. Officers often do not have sufficient preparation to handle issues in a diverse data processing environment.
c. Unknown victims. Most of the time, the victims are collective groups. In the case of individual victims, many of them may not even realize that there is a security issue and therefore do not have the means to respond to incidents of cybercrime.
d. The victims' reluctance to report cybercrimes after discovering them. For companies, especially in the business sector, this reluctance is related to

two dilemmas. First, some victims may be unwilling to disclose information about their operations due to fear of negative publicity, public embarrassment, or loss of goodwill. Second, other victims may worry about the loss of investor or public trust and the economic impact that it may bring.

3. Differences in Legal Systems Between Countries

The harmonization of laws between countries is a major challenge in international cooperation. Each country has its own legal system, definitions of crime, and judicial procedures that differ. What is considered a crime in one country may not be regarded as a crime in another country, or may have a different level of sanctions (Hapsoro, Aidjili & Budijanto, 2022). These differences create legal loopholes that can be exploited by cybercrime perpetrators to evade prosecution. The extradition process also becomes complicated due to the differences in definitions and classifications of crimes between countries.

4. Technical Capacity Limitations

Not all countries have the same technical capacity to deal with cybercrime. Limitations in technology infrastructure, the expertise of human resources, and digital forensic tools pose significant obstacles to international cooperation. Developing countries often face resource limitations in building adequate cybersecurity capacity. This creates a gap in investigative and cybercrime handling capabilities, which can hinder effective international cooperation.

5. The Speed of Technological Development

Technology is developing at a very rapid pace, whereas the process of creating laws and international policies takes a long time. When an international legal instrument is successfully enacted, the technology that served as the basis for the law may already be outdated or have evolved into a different stage (Judijanto & Nugroho, 2025). Cybercriminals continue to develop new and more sophisticated techniques and strategies, while the international legal response tends to be reactive and slow in keeping up with these developments.

B. The Effectiveness of the Budapest Convention in Addressing Cybercrime

1. Advantages of the Budapest Convention

The Budapest Convention has several advantages as an international legal instrument. First, this convention provides a comprehensive framework for the harmonization of cybercrime legislation. Second, this convention facilitates the sharing of experiences and creates relationships that facilitate cooperation in specific cases. This convention can also be used by any country as a guide, checklist, or model law. Being a party to this agreement offers additional benefits in the form of access to more effective international cooperation mechanisms (Khoirunnisa & Jubaidi, 2024).

2. Limitations of the Budapest Convention

Despite its advantages, the Budapest Convention also has limitations. This convention was created about 20 years ago, before the exponential growth of internet usage, the development of cloud computing, and the digitization of almost every type of interaction. Technological changes have made electronic evidence crucial for almost every type of crime, not just cybercrime. This necessitates the updating of the convention to accommodate the latest technological developments.

3. Implementation Challenges

The implementation of the Budapest Convention faces various practical challenges. Not all countries are parties to this convention, which creates gaps in international cooperation. Countries that have not ratified the convention may have no legal obligation to cooperate in addressing cybercrime.

4. Technical and Structural Barriers

Technical barriers in international cooperation to combat cybercrime include limitations in technology infrastructure, lack of standardization of information systems, and difficulties in exchanging digital forensic data between countries. Differences in information technology systems between countries can complicate joint investigation processes. Lack of standardization in data formats and communication protocols can hinder the efficiency of cooperation. Structural barriers include differences in law enforcement organizational structures, suboptimal coordination mechanisms, and a shortage of trained human resources in the field of cybercrime. Each country has a different institutional structure for addressing cybercrime. Some countries have special cybercrime units, while others handle it through conventional crime units. These differences can complicate coordination and communication between countries (Safitra, Lubis & Fakhrurroja, 2023).

C. Indonesia's Position in International Cooperation

Indonesia, as one of the countries with the fastest digital economic growth in Southeast Asia, faces unique challenges in regulating cybercrime. Indonesia has witnessed an exponential increase in internet usage and digital transactions, accompanied by a rise in cyber threats. Despite the implementation of domestic regulations such as the Electronic Information and Transactions Law (UU ITE), there are still gaps in addressing the complexities of transnational cybercrime and ensuring adequate alignment with international standards (Aldriano, & Priyambodo, 2022).

Indonesia has shown a serious commitment to developing national cybersecurity. The establishment of the Cyber and Sandi National Agency (BSSN) is a strategic step to strengthen Indonesia's cybersecurity capacity. Research indicates that the development of Indonesia's cybersecurity has been reinforced by the formation of this special agency, which is responsible for coordinating cybersecurity efforts at the national level. Indonesia's cyber diplomacy has resulted in collaborations with other countries to enhance cybersecurity as part of national security. This cooperation has been conducted bilaterally and multilaterally and can be categorized as cooperative security based on shared goals (Fadhillah, 2023).

Indonesia actively participates in various international forums related to cybersecurity and cybercrime, including ASEAN Cybersecurity Cooperation, collaboration with Australia in the field of cybersecurity, and participation in various multilateral initiatives. Despite various efforts, Indonesia still faces challenges in international cooperation to combat cybercrime. These challenges include the limited number of trained human resources, the need for technological capacity building, and the necessity for legal harmonization with international standards.

Indonesia has not ratified the Budapest Convention, which may be an obstacle in international cooperation. Nevertheless, Indonesia has developed a national legal framework through the ITE Law and various regulations related to cybersecurity (Faturohman, Hidjriana, & Rahayu, 2023). The legislative policy stage is the most strategic phase when it comes to operationalizing criminal sanctions. At this stage, the policy framework for the criminal system and sentencing is formulated, which also serves as the legislative basis for the subsequent stages, namely the stage of criminal enforcement by the judiciary and the stage of execution of penalties by law enforcement officials. Legislative policy in formulating the criminal system also plays an important role in regulating cybercrime in Indonesia.

The regulation of cybercrime in Indonesia materially has two meanings, namely in a broad and narrow sense. In a broad sense, cybercrime includes all crimes involving electronic means or systems, including conventional crimes in the Penal Code such as murder or human trafficking, as long as they utilize electronic systems. Additionally, this regulation also covers crimes regulated under Law No. 3 of 2011 on Fund Transfers, the Banking Law, and Law No. 8 of 2010 on Money Laundering (Hasan, 2022).

In a narrow sense, cybercrime is regulated by Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law) which has been amended by Law No. 19 of 2016. Although it does not provide a direct definition of cybercrime, the ITE Law refers to the classification in the Convention on Cybercrime, which includes crimes involving illegal activities such as the dissemination of illegal content, gambling, defamation, extortion, fake news, and the spread of hatred based on SARA (ethnicity, religion, race, and inter-group relations). Additionally, the ITE Law also covers crimes related to data disruption and electronic systems, electronic document forgery, as well as additional crimes such as aggravated criminal threats.

Indonesia has several regulations governing cybercrime, particularly Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law) which has been amended by Law No. 19 of 2016. However, with the existence of The United Nations Convention Against Cybercrime, there are several implications that need to be considered to strengthen the domestic legal framework. That is, to harmonize the definitions and scope of cybercrime. The UN Convention establishes a more comprehensive definition and scope of cybercrime. This requires alignment in the ITE Law and other related regulations to ensure that all forms of cybercrime regulated under the convention are also covered in domestic law. For example, crimes such as data theft, ransomware attacks, and the misuse of artificial intelligence technology need to be regulated more specifically (Kuncoro, 2016).

The convention requires member states to align their domestic laws with the international standards set out in the agreement. In the context of Indonesia, the ITE Law has become the primary legal basis for addressing cybercrime, such as illegal access, illegal interception, and the distribution of child pornography. However, several aspects of the convention, such as cross-border cooperation in collecting electronic evidence and extraditing cybercriminals, require further

adjustments to the ITE Law and other related regulations. For example, the convention stipulates that member states must be able to request electronic data from internet service providers in other countries during investigations into serious crimes. This necessitates an update of legal mechanisms in Indonesia to comply with fast and reliable international procedures.

CONCLUSIONS AND RECOMMENDATIONS

Based on the analysis that has been conducted, it can be concluded that international cooperation in combating cybercrime faces various complex challenges. The main challenges include the complexity of jurisdiction, differences in legal systems between countries, limitations in technical capacity, and the rapid pace of technological development that is difficult for international legal responses to keep up with. The Budapest Convention, as the main international legal instrument in the field of cybercrime, plays an important role but also has limitations that need to be addressed through updates and adaptations to the latest technological developments. The implementation of this convention still faces various practical obstacles that require innovative solutions. Indonesia has demonstrated a serious commitment to developing national cybersecurity and international cooperation, but there is still a need for capacity improvement and legal harmonization with international standards.

This study recommends the need for Indonesia to strengthen international legal diplomacy, update national cyber regulations, and establish an integrated cyber coordination center with international partners.

ACKNOWLEDGMENT

On this occasion the researcher would like to thank all parties who have helped the researcher in completing this article. Hopefully in the future we can collaborate on more in-depth research.

REFERENCES

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. Judge: Jurnal Hukum, 05(02)

Aldriano, Muhammad Anthony, and Mas Agus Priyambodo. "Cyber Crime Dalam Sudut Pandang Hukum Pidana." Jurnal Kewarganegaraan 6, no. 1 (2022):

Balboni, Paolo and Pelino, Enrico, "Law Enforcement Agencies' Activities in the Cloud Environment: a European Legal Perspective", *Information & Communications Technology Law*, Vol. 22, No. 2, 2013.

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Sunarto, H. B. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya (Desember 2024). Jurnal Kolaboratif Sains, 8(1)

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*. Universitas Padjadjaran

Bunga, M. (2020). Legal Response to Cybercrime in Global and National Dimensions. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, Universitas Padjadjaran.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). Pandecta: Research Law Journal, 13(1)

Fadhillah, Siti Aura, Michelle Sharon Anastasia Matakupan, and Britney Wilhelmina Berlian Mingga. "Peran Interpol Dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest on Cybercrimes." Journal on Education 5, no. 4 (2023)

Fahlevy, M. R., et al. (2025). Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber. *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan*, 6(1).

Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. Kultura: Jurnal Hukum, Sosial, Dan Humaniora, 1(6)

Faturohman, Rachmat Putra Hidjriana, and Rizky Zendra Rahayu. "Dampak Pengaruh Teknologi Terhadap (Cyber Crime) Tindak Pidana Serta Analisis Hukum." … of Constitutional Law … 3, no. 1 (2024): 1–11.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. Jurnal Dinamika Global, 7(02)

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. Jurnal Dinamika Global, 7(02)

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, IPDN.

Hapsoro, W., Aidjili, M., & Budijanto, H. A. (2022). Yurisdiksi Hukum Pidana Dalam Pembatasan Informasi Hoaks Terkait Dengan Kejahatan Cybercrime. RISTEK: Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang, 7(1)

Hasan, Muh.Irfansyah. "KEJAHATAN TRANSNASIONAL DAN IMPLEMENTASI HUKUM PIDANA INDONESIA." Lex Crimen 7, no. 7 (2022):

Hui, Kai-Lung, Seung Hyun Kim, Qiu-Hong Wang, "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks", *MIS Quarterly,* Vol. 41 No. 2, 2017

Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. Sanskara Hukum Dan HAM, 3(3)

Kasturirangan, K., & Shankar, P. (2017). *Cyber Crime and Cyber Security: Legal and Technical Perspectives*. New Delhi: Sage Publications.

Khoirunnisa, K., & Jubaidi, D. (2024). Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. Politeia : Journal of Public Administration and Political Science and International Relations, 2(2)

Kuncoro, Tri. "PENEGAKAN HUKUM TERHADAP CYBER CRIME DI BIDANG PERBANKAN SEBAGAI KEJAHATAN TRANSNASIONAL." Jurnal Magister Hukum Udayana (Udayana Master Law Journal) 19, no. 5 (2016)

Moise, Adrian Cristian, "Some Considerations on the Phenomenon of Cybercrime", *Journal of Advanced Research in Law and Economics*, Vol. 5, Issue 1, 2014.

Moitra, Soumyo D., "Developing Policies for Cybercrime Some Empirical Issues", *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13, Issue 3, 2005.

Rai, I. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 13(1).

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. In Sustainability (Switzerland) (Vol. 15, Issue 18). Tobing, C. I., Surya, T. M., & Selvias, L. R. (2024). Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas. JURNAL HUKUM SASANA, 10(2),

Yasmirah Mandasari Saragih, Post-Genesis Digital Forensics Investigation, International Journal of Scientific Research in Science and Technology (www.ijsrst.com), Volume 3 | Issue 6 | Print ISSN: 2395-6011. July-August-2017 [(3) 6: 164-166].