Legal Analysis of Police Challenges in Facing Transnational Cyber Crime

Rahmat Efendi Tanjung[1], Ahmad Ansyari Siregar[2], Nimrot Siahaan[3*]

[1,2,3]Faculty of Law, Labuhanbatu University, Labuhanbatu, Indonesia
*Coresponding Author:
Email: nimrotsiahaan4@gmail.com

Abstract.

The development of information technology has triggered an increase in transnational and increasingly complex cybercrimes. The cross-border nature of cybercrime poses serious challenges for law enforcement officials, particularly the Indonesian National Police (Polri), in the investigation, arrest, evidence-proving, and law enforcement processes. This study aims to analyze the legal challenges faced by the police in dealing with transnational cybercrime, including limited regulations, differences in jurisdiction between countries, difficulties in obtaining electronic evidence, limited technological and human resource capacity of the police, and limited international cooperation. Using a normative-juridical approach, this article finds that strengthening legal instruments, optimizing digital forensics, increasing investigator capacity, and intensifying international cooperation are strategic steps to increase the effectiveness of cybercrime countermeasures. In conclusion, the challenges faced by the police are multidimensional, requiring an adaptive, collaborative, and technology-based legal response. The normative-juridical approach is used to identify legal gaps based on the Criminal Procedure Code (KUHAP), the ITE Law No. 19 of 2016, and police regulations, which often hinder the collection of evidence and the determination of suspects due to victims being abroad. Recommendations include strengthening international cooperation, human resource training, harmonization of cyber regulations, and collaboration with the private sector for effective law enforcement in the digital era.

Keywords: *Cybercrime; Transnational and Policing.*

I. INTRODUCTION

The development of information technology has transformed patterns of social, economic, and governmental interaction, but has also opened up new opportunities for the emergence of transnational cybercrime. Cybercrime is no longer bound by jurisdictional boundaries, making it difficult for law enforcement officials, particularly the Indonesian National Police (Polri), to investigate, prosecute, and enforce the law. This transnational nature involves perpetrators, victims, and electronic means from various countries simultaneously, thus requiring a modern, integrated legal approach, international cooperation, and high technical capacity.This article discusses a legal analysis of the challenges police face in confronting transnational cybercrime, examining national regulatory aspects, global cooperation mechanisms, obstacles to law enforcement, and strategic solutions to increase the effectiveness of cybercrime countermeasures. Transnational cybercrime is an increasingly complex threat to the Indonesian police force. The main challenges in addressing these crimes include the transnational nature of the crimes, the anonymity of the perpetrators, the volatility of digital evidence, and the limited resources and expertise of investigators in digital forensic technology. These conditions complicate the process of collecting and analyzing valid evidence for use in legal proceedings.One of the key characteristics of modern cybercrime is its transnational nature, where perpetrators, victims, technological tools, and impacts can be located in multiple countries simultaneously.

This situation creates complex legal challenges for police, especially when evidence gathering, digital footprint tracing, or enforcement efforts require the involvement of legal authorities in other countries. National borders are no longer a barrier for cybercrime perpetrators, while for law enforcement, jurisdictional boundaries become a major obstacle. In Indonesia, cybercrime cases continue to increase year after year, encompassing cross-border online fraud, ransomware attacks, hacking, personal data theft, and financial crimes involving international networks. This situation requires the Indonesian National Police, particularly the Cyber Crime Directorate of the Criminal Investigation Agency (Bareskrim), to improve their

capacity, strategy, and legal preparedness to address these global threats.In a normative context, Indonesia actually already has regulations such as the Electronic Information and Transactions Law (ITE Law), Law No. 1 of 2006 concerning Mutual Assistance in Criminal Matters, as well as various other derivative regulations. However, rapid technological developments often mean these regulations lag behind increasingly sophisticated cybercrime methods.

Furthermore, international cooperation is often hampered by differences in legal systems, lengthy MLA processes, and the limited understanding of digital evidence by judicial institutions.Therefore, a legal analysis of the police's challenges in handling transnational cybercrime is crucial as a basis for formulating more effective strategies and policies. This article examines in-depth regulatory aspects, evidentiary barriers, technological and human resource capacity, and the need for international cooperation to strengthen the police's role in countering transnational cybercrime.Transnational cybercrime includes various illegal activities such as hacking, online fraud, data theft, malware distribution, and cyber terrorism. Its distinctive feature is that the perpetrator, victim, server, and digital footprint can be spread across multiple legal jurisdictions. This situation makes it impossible to handle it with conventional national legal approaches. The Indonesian National Police, represented in this case by the Cyber Crime Directorate (Dittipidsiber) of the National Police Criminal Investigation Agency (Bareskrim Polri), is required to adapt to the dynamics of this borderless crime.Transnational cybercrime has become a serious threat to Indonesia's national security along with the rapid development of information technology, with Indonesia contributing around 2.4% of global cybercrime and experiencing a significant increase compared to the previous year.

These crimes include online fraud, the distribution of provocative content, ransomware, and mass data leaks such as the Tokopedia case (96 million users) and government websites, which often involve transnational perpetrators and cause trillions of rupiah in losses. The Indonesian National Police (Polri) faces legal challenges due to the transnational nature of these crimes, such as jurisdictional difficulties, the anonymity of perpetrators through encryption, and the volatility of digital evidence that requires sophisticated forensics. Regulations such as the 2016 Electronic Information and Transactions Law No. 19 and the Criminal Procedure Code have not fully addressed the issue of international cooperation and the limited human resources of investigators. However, law enforcement efforts against transnational cybercrime face a difficult path fraught with fundamental legal challenges. National laws, limited by territorial boundaries, often prove ineffective when confronted with the borderless realities of cyberspace. Jurisdictional conflicts, regulatory gaps, and slow and convoluted international cooperation mechanisms are some of the main obstacles. Therefore, this article aims to analyze these legal challenges in depth and map out the strategic solutions needed to enable the police to optimize their role in maintaining national cybersecurity amidst the currents of digital globalization.

II. METHODS

This research uses a normative legal approach that emphasizes the analysis of applicable laws and regulations, such as the 2016 Electronic Information and Transactions Law No. 19, the Criminal Procedure Code (KUHAP), and police regulations related to handling cybercrime. This research is descriptive and analytical in nature, aiming to systematically outline the legal challenges through legal problem-solving. Primary data sources consist of laws, court decisions, and official National Police documents, while secondary data include books, legal journals, and reports on transnational cybercrime cases. Data collection techniques were carried out through literature studies and document analysis, using qualitative analysis methods to interpret legal gaps and recommendations.

This research is a normative legal research using several approaches, namely:

1. Statute Approach
   Analyze regulations related to cybercrime, such as the ITE Law, the Criminal Procedure Code, the MLA Law, as well as international regulations such as Interpol and ASEANAPOL.
2. Conceptual Approach
   Examines the concepts of cybercrime, digital forensics, jurisdiction, and international cooperation.

3. Case Approach
   Using several cases of cross-border cybercrime to examine the implementation of the law and the obstacles faced by the police.

The research data sources consist of:

a. Primary legal materials:
   Laws, government regulations, police regulations, international conventions, and court decisions.
b. Secondary legal materials:
   Books, law journals, scientific articles, and expert opinions on cybercrime and international jurisdiction.
c. Tertiary legal materials:
   Encyclopedias, legal dictionaries, official reports of international institutions.

Data collection technique :

Data was collected through literature study techniques on:

a. Legal literature
b. Regulatory documents
c. Official reports from the Indonesian National Police, Interpol, and international institutions
d. Previous research publications

III. RESULT AND DISCUSSION

Based on a normative legal analysis of primary and secondary legal materials, this study identifies and discusses four main legal challenges faced by the Indonesian Police in handling transnational cybercrime.

1. Cybercrime Regulatory Framework in the Indonesian Legal System

The research results show that Indonesia already has several regulations governing cybercrime, particularly the ITE Law, the Criminal Procedure Code, and Law No. 1 of 2006 concerning Mutual Assistance (MLA). Although this normative framework provides a legal basis, the rapidly evolving nature of cybercrime has created a legal gap between regulations and modern crime modes. The ITE Law largely regulates acts that can be categorized as cybercrime, but does not specifically regulate:

a. AI-based crimes (deepfake, AI fraud)
b. Global ransomware attack
c. Cross-border crypto financial crime
d. Comprehensive personal data protection arrangements

The absence of specific regulations for transnational cybercrime means that the police must rely on a combination of various rules, including international treaties, which are often not binding. This creates legal uncertainty and slows down the investigation process.

2. Jurisdictional Challenges in Handling Transnational Cybercrime
   Research has found that the main problem for the police is that their jurisdiction is limited to the territory of the Unitary State of the Republic of Indonesia (NKRI), while cybercrime occurs across borders. Perpetrators are often located in other countries, while servers, victims, and digital evidence are spread across different jurisdictions.

Jurisdictional issues include:

1. Difficulty requesting server data located abroad.
   Certain countries have strict privacy regulations, making it difficult for Indonesian police to obtain logs, digital footprints, or customer data.
2. Slow MLA (Mutual Legal Assistance) process.
   MLA applications require a lengthy administrative process, making them highly ineffective for time-sensitive digital evidence.
3. Not all countries cooperate.
   Indonesia is not a member of the Budapest Convention, so its access to international cooperation is limited compared to countries that have ratified the convention.

As a result, many international cybercrime cases cannot be resolved or take a long time, so the chances of catching the perpetrators are getting smaller.

3. Obstacles to Evidence and Digital Forensics

   The results of the study show that providing evidence in cybercrime is a major challenge because all evidence is electronic and easily deleted.

Obstacles to proof found include:

a. Digital data volatility, so that evidence can disappear in a matter of seconds.
b. High level encryptionmaking it difficult for investigators to access devices or files.
c. Lack of uniform digital forensic standardsbetween countries.
d. Global platforms like Facebook, Google, and Telegram have different legal procedures for data disclosure, often out of sync with Indonesian law.

In addition, investigators at the regional level (regional police/regency police) often lack digital forensic facilities and must send evidence to the central government, causing the handling process to drag on.

4. Limitations of Human Resources and Police Technology

   Research has found that police human resources' capabilities in cybercrime still need to be improved. Although the Criminal Investigation Agency (Bareskrim) has a fairly advanced cyber unit, not all regions have expert digital forensic investigators.

Limitations found include:

a. The number of expert cyber investigators is still minimal, while the volume of cases is very high.
b. Lack of training related to reverse engineering, malware analysis, blockchain forensics, and cryptocurrency tracing.
c. Digital analysis equipment is unevenly distributed across regions.
d. Cybercrime perpetrators use more advanced technology than the authorities.

This condition widens the “technology gap” between cybercriminals and the police.

5. Suboptimal International Cooperation

   Transnational cybercrime is impossible to tackle without international collaboration. However, research shows that there are still obstacles to police cooperation with other countries.

Some of the obstacles encountered:

a. Differences in legal systems cause responses between countries to be inconsistent.
b. There is no regional cyber command center in Southeast Asia that can provide early warning.
c. Communication between countries is often hampered by bureaucracy.
d. Not all countries are willing to provide user data due to strict privacy regulations.

However, to handle crimes such as global ransomware, international carding, and dark web-based human trafficking, a fast and flexible collaborative network is required.

6. Strategies and Solutions to Increase the Effectiveness of Law Enforcement

   The research results concluded a number of strategic steps that can be implemented by the police:

1. Comprehensive cybercrime regulatory reform, including amendments to the ITE Law and strengthening of electronic evidence regulations.
2. Digital forensics capacity building, both in terms of personnel and equipment.
3. Building a Cyber Fusion Centerwhich integrates the Indonesian National Police, Ministry of Communication and Information, BIN, BSSN, OJK, and other institutions.
4. Encourage Indonesia to join the Budapest Conventionto expand access to law enforcement cooperation.
5. Increase cyber patrolto monitor the movements of perpetrators on the dark web and global digital space.
6. Strengthening digital security education in societyto reduce the number of victims.

With these various strategies, the effectiveness of handling cybercrime can be significantly increased.

Some of the increasingly dominant modes include:

1. Ransomware-as-a-Service (RaaS)
   The perpetrators provide the ransomware platform to other operators who want to attack computer systems in any country. This complicates the investigation because the main perpetrator and operators are located in different countries.
2. Targeted Global Phishing (Spear Phishing International)
   Perpetrators target victims in various countries with very specific social manipulation and use AI to imitate a person's voice or face (deepfake).
3. Cryptocurrency Laundering
   Criminal funds are laundered through blockchain, mixer services, or anonymous overseas wallets, making it difficult for Indonesian police to track them.
4. Dark Web Marketplace
   The sale of narcotics, credit card data, personal data, and even weapons is carried out on dark forums whose servers are located in various countries.

This method makes it difficult for the police to determine who the perpetrator is, where the crime took place, and which country should process the case legally.Harmonization of national laws with global standards, including the creation of a special law for cybercrime, is needed to close the legal gap, supported by forensic training and cooperation between BSSN and Polri. Preventive efforts through the ITU's cybersecurity pillars, such as organizational coordination and capacity building, could improve Indonesia's ranking from 77th in the GCI.This complexity is rooted in the borderless nature of the cyber world, while laws were created for the territorial physical world. The Indonesian National Police, which by default operates on a territorial basis, often encounters a dead end when investigations must cross national borders. For example, requests for access to server logs from cloud service providers headquartered overseas cannot be processed simply with a standard Investigation Warrant (SPHP) but must instead go through a lengthy Mutual Legal Assistance (MLA) procedure. This jurisdictional conflict is exploited well by criminals (jurisdictional arbitrage) by choosing to operate from countries with weak cyber laws or limited international cooperation. As a result, police efforts often only succeed at blocking access by the Ministry of Communication and Information, but fail to arrest the main perpetrators who are outside the jurisdiction.

Table 1. Limitations of Police Human Resources and Technology

No	Main Weaknesses	Explanation	Impact on Law Enforcement
1	Shortage of digital forensics experts	Cyber investigators are still limited in number	Late case handling
2	Uneven equipment	Police/Regional Police do not have digital analysis tools	Evidence must be sent to the center
3	Lack of further training	Malware analysis, blockchain forensics, AI crime	Investigators are slower than the perpetrators
4	High workload	The number of cases increases every year	The effectiveness of investigations decreases

This regulatory challenge is two-fold. First, there is a substantive gap. The ITE Law does not explicitly define ransomware attacks as aggravated extortion, cryptojacking, or the use of AI for deepfake fraud. This forces investigators to resort to vague articles or analogies, which are legally risky and subject to challenge in court. Second, there is the evidentiary challenge. Although the ITE Law recognizes electronic evidence, in practice, the digital chain of custody standards applied by courts are often very high and technical. Investigators must convincingly prove that seized digital data has not been altered from the time it was taken until it was presented in court, a challenge that is particularly difficult if the data originates from servers across borders. This regulatory lag places the police in a constant "catch-up" situation with the technological advancements of criminals.

Table 2. Cybercrime Handling Solution Strategy

No	Strategy	Explanation	Positive impact
1	Strengthening cyber regulations	Revision of the ITE Law and electronic evidence regulations	The police have a strong legal basis
2	Improving digital forensics capabilities	Training, analysis tools, and cybersecurity lab	Digital evidence is easier to find
3	Join the Budapest Convention	Expanding international cooperation	Accelerate the exchange of data and evidence

4	Establishment of Cyber Fusion Center	Integration of the Police, BSSN, OJK, Kominfo	Faster and more coordinated handling
5	Cyber patrol and early detection	Monitor the dark web and attack patterns	Prevention is more effective

IV. CONCLUSION AND SUGGESTIONS

Conclusion

The Indonesian police face major legal challenges in handling transnational cybercrime due to its cross-border nature, the anonymity of perpetrators, the volatility of digital evidence, limited human resources, and regulations such as the Electronic Information and Transactions (ITE) Law that have not fully adapted to technological developments. These gaps contribute to low investigative and evidentiary effectiveness, as evidenced by the mass hacking and ransomware cases that have placed Indonesia at a high global cybercrime ranking.

Suggestion

1. Strengthening National Regulations
   The government needs to update and synchronize regulations related to cybercrime, including revisions to the ITE Law, the Criminal Procedure Code, and personal data protection regulations to be more responsive to the latest forms of cybercrime.
2. Improving Investigator Competence
   The Indonesian National Police (Polri) needs to expand intensive training in digital forensics, information technology, digital tracking, encryption, and cyber investigation to improve the professionalism of investigators.
3. Digital Forensics Optimization
   Procurement of advanced and standardized digital forensic equipment is a priority to support the process of proving and validating electronic evidence.
4. Strengthening International Cooperation
   The Indonesian National Police (Polri) needs to expand its cooperation network with Interpol, AseanPOL, and other international institutions through joint investigation, extradition, and mutual legal assistance mechanisms.

REFERENCES

[1] Al-ulamai, Ulil Amri, Rustam Dahar, Karnadi Apollo, and Ali Maskur. “Challenges of Law Enforcement Against Cybercrime in the Digital Era in Central Java” 18, no. 02 (2025): 249–57.

[2] Influential, Which, On Stability, and Country Year. No Title. Vol. 2024, 2025.

[3] Ghiffari, Abizar Al. “Cybercrime and the Challenges of Law Enforcement in Indonesia Coordination with Criminal Enforcement When Data Leak Cases Intersect with Cross-Border Evidence Action, Especially When Attack Infrastructure Such as Servers, Domains, or Wallets in the Digital Social and Cultural Realm, Analysis of Public Discourse on Online Social Media, Investment Fraud, and Hate Speech (Kusnadi et al., 2025). The Data Can Be Enforced, As Well As Being Material for Formulating More Digital Literacy Education Policies” 02, no. 02 (2025): 1295–99.

[4] Faculty of Law. “The Role of the Police in Law Enforcement Against Cyber Crime Giviyandi Saragih,” nd, 1–10.

[5] Law, Policy, Criminal Law Against, Cyber Crime, Comparison Between, Indonesia and, International Law Perspective, Between Indonesia, and International Law. “Aulia Mawaddah Matondang and Andryan, Muhammadiyah University of North Sumatra” 6, no. 1 (2025): 1–14.

[6] Islam, Family Law, and Article Info. “Evidence Challenges in Cybercrime Cases” 05, no. 02 (2024): 55–63.

[7] Islam, University, and Nusantara Bandung. “Rewang Rencang: ***Jurnal Hukum Lex Generalis***. Vol.6. No.7 (2025) Theme/Edition: Criminal Law (Seventh Month) Https://Jhlg.Rewangrencang.Com/” 6, no.7 (2025): 1–26.

[8] Maruli, Sahat, Tua Situmeang, and Krusitha Meilan. “The Evolution of Crime and Punishment: Challenges in Law Enforcement and Modern Penology” 7, no. 2 (2025): 87–97.

[9] Perspective, From, and Criminal Law. “***Juridical Analysis of the Increase in Cyber Crime Acts Reviewed”*** 2, no. 3 (2024): 1434–45.

[10] Putra, Steven Sanjaya, and Shera Aurelia Kusoy. “A Legal Analysis of Phishing Cybercrime Prevention in Indonesia” 3, no. 4 (2025).

[11] Study, Program, Legal Studies, Faculty of Sharia, AND Law, UIN Syarif, and Hidayatullah Jakarta. “Law Enforcement Against Perpetrators of the Crime of Dumping B,” 2022.

[12] Sunan, UIN, and Kalijaga Yogyakarta. “Legal Protection and Prevention of Cybercrime in the Digital Era in the Indonesian Legal System Rahma Agri Firdaus Introduction Cybercrime is a branch of criminal law that specifically regulates crimes committed using information and communication technology (ICT), especially the internet. Cybercrime, also known as cybercrime, includes various illegal activities that utilize computers, computer networks, and other digital devices. The scope of cybercrime law covers various aspects related to the regulation, prevention, investigation, and prosecution of cybercrime, often referred to as computer violations. Hamzah defines cybercrime as "crimes in the field of computers in general can be interpreted as the illegal use of computers" 2 , while Wisnubroto in his book defines computer crime as an unlawful act committed using a computer as a means or tool or computer" 4, no. 1 (2024).

[13] Tirtayasa, Yustisia, Desia Rakhma Banjarani, and Muhammad Apriliansyah Rahmadhani. “Cybercrime as a Transnational Crime: Law Enforcement and Cybercrime Prevention in the Perspective of International Criminal Law Keywords Abstract Keywords” 4, no. 4 (2024).

[14] Tobing, Clara Ignatia, Tiofanny Marylin Surya, and Liris Roesa Selvias. “Digital Globalization and Cybercrime: Legal Challenges in Facing Cross-Border Cybercrime” 10 (2024): 105–23.