LEGAL JURISDICTION AND PLACE OF OCCURENCE IN TRANSNATIONAL CYBERCRIME: A NORMATIVE ANALYSIS OF GLOBAL LAW AND INDONESIAN TELECOMMUNICATIONS REGULATIONS

Agustinus Nicholas L Tobing[1*], Annisa Fitria[2]
[1,2]Faculty Law, Universitas Indonesia Esa Unggul Jakarta, West Jakarta, Indonesia
augie.nicholas@student.esaunggul.ac.id[1*], fh@esaunggul.ac.id[2]

Received 30 Nov 2025 • Revised 27 Dec 2025 • Accepted 16 Jan 2026

Abstract

This study investigates the establishment of legal authority and the site of the offense in international cyber offenses via a normative legal method, emphasizing global legal viewpoints such as the Budapest Convention, UN Convention against Cybercrime 2024, and Tallinn Manual 2.0, along with Indonesia's domestic information technology laws including Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) with its revisions, and Law No. 27 of 2022 on Personal Data Protection (UU PDP). The foundation stems from the rising worldwide cyber risks that transcend borders, with BSSN records noting over 5,000 occurrences in Indonesia in 2025, while the issue formulation encompasses the layered definition of the site of the offense and cross-country investigative authority based on global concepts and examples like cyber assaults on Taiwan (2024-2025), INTERPOL reports on African cyber offenses (June 2025), and INTERPOL financial activities (September 2025). The research approach includes gathering secondary materials such as legal texts and official documents, employing statutory, comparative, and case evaluations to yield practical suggestions like ratifying international conventions, developing judicial guidelines, and establishing a national task force. The outcomes highlight the adjustment of authority theories for intangible cyber spaces, including three site of offense concepts (locus actus, effectus, instrumentum), and advocate for alignment to address regulatory voids, provide assurance, and safeguard state interests in the digital age.

Keywords: Locus Delicti, Jurisdictions, International Law

INTRODUCTION

Advances in information and communication technology have created a new arena for human interaction known as cyberspace. This environment not only facilitates transactions and communication between countries, but also opens up opportunities for new forms of violations that transcend jurisdictional boundaries, such as system hacking, the spread of malicious software, theft of personal information, and digital espionage (Djanggih & Qamar, 2018). This phenomenon highlights the importance of legal analysis regarding the determination of jurisdiction and the location of the crime in transnational cybercrimes, especially when the perpetrator, victim, and attacked system are located in different countries.

Legal issues arise in relation to the limitations of applying national criminal law to acts committed in cyberspace. In practice, law enforcement officials often face challenges in determining where cybercrimes are considered to have occurred (Pakaya & Mahyani, 2022) and which country's laws have jurisdiction over them (Galih, 2019). This situation leads to overlapping jurisdictions and potential conflicts of authority between countries (Ibold, 2020).

In addition, there are various issues related to the inconsistency between domestic regulations and global laws. Indonesia already has a legal framework in place, such as the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), but these two regulations are not yet fully aligned with international norms such as the Budapest Convention on Cybercrime and the United Nations Convention against Cybercrime (2024) (Assembly, 2024; Budapest, 2001). Delays in the ratification and harmonization of domestic regulations are an obstacle to global collaboration, especially in efforts to transfer suspects and exchange digital data between countries (Widiastuti & Saragih, 2025).

The main statement of this study is that the determination of jurisdiction and the location of the crime in cross-border cybercrime cannot be limited to physical space alone, but must consider virtual aspects and legal consequences (effects doctrine) that arise across national borders (Huang, 2024). Thus, the appropriate legal approach is through the application of concurrent jurisdiction, namely the recognition that more than one country can have jurisdiction over a single cybercrime, as long as there is a valid legal connection (Maillart, 2019; Ryngaert, 2025).

Supporting this statement is the nature of cybercrime, which knows no boundaries, rendering conventional territory-based law enforcement mechanisms inadequate. It is necessary to reformulate the concept of the scene of the crime to emphasize not only the location where the perpetrator committed the act, but also the location where the impact occurred and the location of the server or data that was attacked (Purwaningsih & Putranto, 2023).

Based on data from the United Nations Office on Drugs and Crime (2013), more than 60% of transnational cybercrime cases fail to be resolved due to jurisdictional barriers and limited cooperation between law enforcement authorities. In Indonesia itself, cases such as online fraud, data extortion attacks, and information leaks show that domestic legal instruments are not yet capable of responding to the challenges of cross-border law enforcement (Rusydi, 2025).

Based on this explanation, the research questions in this study are as follows: 1) How are the definition and mechanism for determining the location of a crime in cross-border cybercrime interpreted based on global legal principles and telecommunications law provisions in Indonesia? 2) Which country's jurisdiction leads the investigation of multi-jurisdictional cybercrimes based on international concepts and case studies?

RESEARCH METHOD

The research method used in this study is a normative juridical approach, which examines primary and secondary legal materials through literature study. The analysis is conducted descriptively and analytically to interpret global legal principles and their application in the context of Indonesian national law (Marzuki, 2019).

RESULTS AND DISCUSSION

International Legal Jurisdiction Theory

The concept of authority in global law is not the creation of a single individual, but rather developed gradually from customary law principles and international court decisions in the early 20th century with the SS Lotus case (1927) by the Permanent Court of International Justice (PCIJ) often considered the main basis for establishing the principle that states can exercise authority as long as it is not prohibited by international law, influenced by the thinking of experts such as Alberico Gentili (1552–1608) as the pioneer of the secular school of global law (Colangelo, 2009; Ryngaert, 2025; Tzouvala, 2015). This contemporary doctrine was later developed by Frederick A. Mann through his

work in the 1980s, which provided an in-depth analysis of prescriptive, executive, and adjudicative authority (Ryngaert, 2025). The concept of authority in international law is based on fundamental principles codified in customary law and treaties, including the principle of territory (crimes within a state's territory), active nationality (the nationality of the perpetrator), passive nationality (the nationality of the victim), protective (protection of vital interests), and universal (universal crimes such as cyber terrorism) (Nyoto, 2021; Schmitt, 2017; Widiastuti & Saragih, 2025). In the cyber sphere, this concept is adapted to accommodate the non-physical nature of the scene of the crime, where jurisdiction may be shared based on the location of the server, the perpetrator, or the impact, as explained in the Tallinn Manual 2.0 Rule 1-10 on cyber sovereignty and Rule 30-40 on attribution (Schmitt, 2017). As an example of shared jurisdiction, the case of an online fraud syndicate in Cambodia in October 2025 involved 110 Indonesian citizens as victims/perpetrators, where Indonesia claimed active citizenship jurisdiction (perpetrators were Indonesian citizens) while Cambodia claimed territorial jurisdiction (crime committed in its territory), thus requiring bilateral cooperation through ASEAN for resolution (Permana, 2025). Attribution is an important element, requiring forensic evidence to link state actors to attacks, thereby avoiding diplomatic conflicts, as in the case of the attribution of data extortion attacks in 2025 (Budapest, 2001; Putri Ramli A. F.).

In practical terms in Indonesia, this concept is implemented through Article 2 of the ITE Law, which allows for extraterritorial jurisdiction if the impact is felt within the territory of the Republic of Indonesia, such as in the case of transnational fraud, which is expected to increase by 70% in 2025 (BSSN data), where the Indonesian National Police can lead the investigation even if the perpetrators are located overseas, with the cooperation of INTERPOL for attribution. The protective principle is applied by BSSN in protecting critical infrastructure, for example, in response to DDoS attacks, which are expected to increase by 40% in 2025, in line with Tallinn Manual Rule 4 to prevent foreign intervention. This implementation requires improved digital forensic capabilities, such as training for prosecutors to use server log evidence, to overcome domestic authority limitations in a global context such as AI fraud in Southeast Asia (Crime, 2025).

This concept also includes the principle of "aut dedere aut judicare" (extradition or prosecution), which is relevant to cybercrimes where the perpetrator is located in another jurisdiction, as applied in the Budapest Convention (Budapest, 2001). Although historically associated with serious crimes such as terrorism, this principle has been adopted in cybercrime conventions to ensure that impunity can be avoided through the alternatives of extradition or domestic prosecution, as explained in the Explanatory Report to the Budapest Convention (Paragraph 6). A more descriptive alternative term is 'extradite or prosecute', which emphasizes the obligation of states to choose one without leaving any legal loopholes. In Indonesia, this concept has been adapted through the extraterritorial principle in Article 3 of the KKS Bill, which emphasizes legal protection against cross-border cyber impacts (Law Number 27 of 2022 Concerning Personal Data Protection, 2022; Nugroho & Chandrawulan, 2023).

Locus Delicti

To determine the location of a transnational cybercrime, particularly in Indonesia, three main concepts are applied: the concept of the location where the crime was committed (locus actus), the concept of where the consequences of the crime arise (locus effectus), and the concept of the tools used to commit the crime (locus instrumentum). The concept of locus actus focuses on the location where the criminal act was committed, such as the location of the perpetrator when sending malicious software; locus effectus focuses on the location where the impact of the crime occurred, such as the country where data was stolen or systems were disrupted; and locus instrumentum focuses on the tools or infrastructure involved, such as the servers or networks used. These concepts form the basis for interpreting the scene of the crime because the virtual nature of cybercrime makes it difficult to physically determine the scene of the crime, thus requiring adjustments to criminal law for better reform (Purwaningsih & Putranto, 2023). An example of a crime scene: In a case of hacking against an Indonesian company by perpetrators abroad in 2024, the locus actus is the perpetrator's country, the locus effectus is Indonesia as the location of the economic loss, and the locus instrumentum is the cloud server in Singapore used as an intermediary, so Indonesia can claim jurisdiction based on the locus effectus in accordance with Article 2 of the ITE Law (Purwaningsih & Putranto, 2023). In a case of carding (credit card theft) in Indonesia in 2025, the locus actus is the location of the perpetrator abroad, the locus effectus is the financial loss in Indonesia (a total of Rp 29.7 billion in cybercrime losses), and the locus instrumentum is a digital platform such as the dark web, allowing the Indonesian National Police to apply Article 30 of the ITE Law for illegal access (Prakasa, 2024).

In practical terms in Indonesia, this concept is implemented through integration with Article 46 of the Personal Data Protection Law, which requires data breaches to be reported within 72 hours,

allowing the locus effectus to be determined based on the impact on Indonesian citizens, such as in the case of carding, which was rampant in 2025 and caused billions of rupiah in losses (according to a report by the Indonesian National Police). BSSN uses locus instrumentum to track foreign servers in investigations, such as DDoS attacks on government websites, which increased by 50% in 2025, where the virtual crime scene is determined via log analysis to support the bilateral extradition process. This application requires reforms, such as the addition of forensic protocols in the KKS Bill, to overcome difficulties in determining the scene of the crime in crypto ecosystem cases where perpetrators are often anonymous (as reported by APIIHI in 2025).

However, in the context of multi-jurisdictional cloud computing, the interpretation of the location of the incident must be done carefully so as not to equate the location of the server directly with the jurisdiction, because cloud servers are often spread across countries and are not subject to a single authority. The Tallinn Manual 2.0 (Schmitt, 2017) distinguishes between jurisdiction of territory (based on the physical location of infrastructure, such as Rule 1 on sovereignty over cyber infrastructure within a country's territory) and jurisdiction of control (effective control over data or operations, which allows for jurisdiction outside the territory if there is an impact or access, such as Rules 8-10). Similarly, Colangelo emphasizes that in cyberspace, authority often creates a 'false conflict' if it relies too heavily on physical territory; instead, jurisdiction of control (who controls the data, e.g., cloud service providers under their national laws) is more relevant than jurisdiction of territory (server location alone), thereby avoiding impunity in cases of data without territory. This adaptation is important in Indonesia, where Article 2 of the ITE Law adopts extraterritorial effects, but needs to be strengthened in the KKS Bill to address multi-territorial clouds through global cooperation.

Relevant Legal and Regulatory Framework

The Budapest (2001) consists of 48 articles regulating substantive crimes (Articles 2-11, such as illegal access and data corruption), investigation procedures (Articles 14-21, including data preservation), jurisdiction (Article 22, allowing joint claims), and international cooperation (Articles 23-35, through MLA and 24/7 networks) (Europe). The UN Convention against (Assembly, 2024) complements this with a focus on prevention (Articles 7-12), investigation (Articles 24-29), and cooperation (Articles 40-46), with an emphasis on human rights despite criticism over potential over-surveillance, and as of October 2025, it has not yet been opened for signature (Nations). In Indonesia, the ITE Law and PDP Law propose a national cyber agency for coordination, with a target completion date of this year (Indonesia, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions; Indonesia, Law No. 27 of 2022 on Personal Data Protection). General international law such as the UN Charter (Article 2(4) on non-intervention) also applies, especially to state-sponsored attacks such as those on Taiwan (Budapest, 2001; Schmitt, 2017).

Case Study Analysis

To provide a complete overview of the three case studies discussed, the following is a summary table presented in Table 1, expanded with a column titled "Relevant Statistical Data." This column includes factual quantitative metrics such as the number of attacks, cost of losses, or operational results, based on official reports and the latest data (as of October 2025). This table is compiled from reliable sources and linked to the concept of authority for ease of understanding.

Table 1. Summary of Transnational Cybercrime Case Studies

Case Study	Main Description	Connection to Jurisdiction Theory	Relevant Statistical Data
Cyberattacks against Taiwan (2024-2025)	Daily attacks have increased to 2.4 million, targeting governments and critical infrastructure, involving cross-border espionage that violates Articles 2-3 of the Budapest Convention and Tallinn Manual Rule 32 (Budapest, 2001; Schmitt, 2017).	Protective jurisdiction for Taiwan with attribution to China, triggering US diplomatic sanctions.	Increase in daily attacks: 2.4 million; Economic impact: billions of dollars (CSIS report).
INTERPOL Report on Cybercrime in	The highest number of ransomware detections in South Africa (17,849 cases) and Egypt (12,281), involving actors from Europe and	Universal jurisdiction through INTERPOL with	Ransomware increase: 50% since 2024; Highest

Africa (June 2025)	Asia, were categorized as transnational incidents violating Articles 6-8 of the Budapest Convention and Article 7 of the UN Convention (Assembly, 2024; Budapest, 2001).	global cooperation for asset recovery.	cases: 17,849 in South Africa.
INTERPOL Financial Crime Operation (September 2025)	The recovery of USD 439 million from a fraud scheme, including USD 6.6 million in assets in Thailand, involved a network spanning Asia, Europe, and Africa, constituting transnational organized crime that violates the protective principles of Article 22 of the Budapest Convention (Budapest, 2001).	Joint jurisdiction through bilateral cooperation for the prevention of cyber money laundering.	Asset recovery: USD 439 million; Specific assets in Thailand: USD 6.6 million.

First case study

Cyberattacks against Taiwan by groups from China in 2024-2025, with daily attacks increasing to 2.4 million, primarily targeting government systems and critical infrastructure. This involves transnational espionage, violating Articles 2-3 of the Budapest Convention on illegal access and Tallinn Manual Rule 32 on cyber espionage (Budapest, 2001; Schmitt, 2017). Protective jurisdiction applies to Taiwan, with attribution to China triggering US diplomatic sanctions. Implications for Indonesia: Similar to threats to regional infrastructure, requiring a KKS bill for resilience, especially after similar incidents in Southeast Asia in 2025 (Law Number 27 of 2022 Concerning Personal Data Protection, 2022). In-depth analysis shows that these attacks highlight the vulnerability of the diplomatic supply chain, with digital forensic recommendations in accordance with PDP Law Article 46, where factual evidence from the CSIS report shows an economic impact of billions of dollars (Galih, 2019; Schmitt, 2017; Putri Ramli A. F.).

Second case study

INTERPOL report on the sharp increase in cybercrime in Africa in June 2025, with the highest number of ransomware detections in South Africa (17,849) and Egypt (12,281), involving many transnational actors from Europe and Asia. This is categorized as a transnational incident because the perpetrators are often from outside the continent, violating Articles 6-8 of the Budapest Convention and Article 7 of the UN Convention on ransomware (Assembly, 2024; Budapest, 2001). Universal jurisdiction is applied through INTERPOL, with global cooperation resulting in asset recovery. For Indonesia, similar to the Asian trend, alignment with the UN Convention is required for global attribution, especially after a decline in local incidents in 2024 but an increase in 2025 (Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions, 2024). This discussion covers the impact on privacy, in line with the UN Convention's criticism of human rights, where INTERPOL data shows a 50% increase in ransomware since 2024 (Assembly, 2024; Widiastuti & Saragih, 2025).

Third case study

INTERPOL's transnational financial crime operation in September 2025 recovered USD 439 million from a fraud scheme, including USD 6.6 million in assets in Thailand, involving networks from Asia, Europe, and Africa. This involved transnational organized crime organizations, violating the protective principles in Article 22 of the Budapest Convention (Budapest, 2001). Joint jurisdiction through bilateral cooperation has implications for Indonesia in the prevention of cyber money laundering, especially after similar cases in the ASEAN region (Law Number 27 of 2022 Concerning Personal Data Protection, 2022). The analysis highlights the need for the KKS Bill for similar international coordination in Southeast Asia, with factual evidence from asset recovery demonstrating the effectiveness of MLA (Assembly, 2024; Fachri, 2022).

Discussion

Definition and Mechanism for Determining Locus Delicti in Transnational Cybercrime

The definition of locus delicti or crime scene in transnational cybercrime is interpreted as a layered location that is not limited to a single physical place, but includes virtual elements such as the

perpetrator's position, the hacked server, and the location where the impact or damage is felt. Based on global legal principles, the crime scene can be defined through the principles of territory and effect, as outlined in Article 22 of the Budapest Convention, which states that jurisdiction applies if the crime is committed in the territory of a country or affects its interests, even if the cyber elements are dispersed (Budapest, 2001). Factual evidence from the 2025 attack on Taiwan, in which perpetrators in China targeted servers in Taiwan with an impact in the US (via allies), shows that the crime scene is not only China (perpetrator's location) but also Taiwan (direct effect) and the US (protective impact), in line with Tallinn Manual Rule 1 on cyber sovereignty, which recognizes the crime scene as multifaceted to avoid impunity (Schmitt, 2017). In Indonesia, the mechanism for determining the scene of the crime is regulated in Article 2 of the ITE Law, which adopts the principle of extraterritorial effects if the crime affects Indonesian territory or citizens, as in the case of data breaches by ShinyHunters in 2025 that affected Indonesian users through global servers (Law Number 11 of 2008 on Electronic Information and Transactions, 2008). BSSN 2025 data shows that 40% of cyber incidents in Indonesia involve foreign servers, so the crime scene is determined through digital log analysis and forensic attribution, in accordance with Article 3 of the KKS Bill, which emphasizes outside the territory for legal certainty (Law Number 27of 2022 on Personal Data Protection, 2022). The relationship between this data and the concept is that the principle of universality in Article 40 of the UN Convention allows for a global crime scene for crimes such as ransomware, as reported by INTERPOL Africa in 2025 with 17,849 cases in South Africa, where the crime scene included perpetrators in Russia and impacts in Africa (Assembly, 2024). This mechanism provides legal certainty by avoiding conflicts of jurisdiction, as evidenced by the recovery of USD 439 million in assets in the September 2025 INTERPOL operation, where the TKP was determined through forensic cooperation (Fachri, 2022). Overall, this definition of crime scene is in line with general international law such as Article 2(4) of the UN Charter, which prohibits cyber intervention, and in Indonesia it is reinforced by Article 46 of the PDP Law on incident reporting, ensuring that crime scenes are determined based on factual evidence such as server logs in the case of Sepah Bank Iran in June 2025 (International Commission of Jurists, 2023; Pakaya & Mahyani, 2022; Purwaningsih & Putranto, 2023; Schmitt, 2017).

Jurisdiction Leading the Investigation and Prosecution in Multi-Jurisdictional Cases

The jurisdiction that should normatively lead investigations and prosecutions in multi-jurisdictional cybercrime cases is the country with the strongest connection to the crime scene, such as the country where the main effects occurred or where evidence is available, with coordination through global cooperation to avoid conflicts. Based on Article 22 of the Budapest Convention, shared jurisdiction allows the state of territory (where the crime was committed) or passive nationality (the victim) to take the lead, as evidenced by the September 2025 INTERPOL operation in which Thailand led the recovery of USD 6.6 million in assets due to local effects, while cooperating with other countries to attribute transnational perpetrators (Budapest, 2001). Factual evidence from INTERPOL Africa's June 2025 report shows South Africa leading ransomware investigations due to the highest number of cases (17,849), in line with the protective principle in Tallinn Manual Rule 4, where countries with impacted infrastructure have priority to maintain sovereignty (Schmitt, 2017). In Indonesia, Article 3 of the KKS Bill and Article 2 of the ITE Law establish national jurisdiction if the impact is felt within the territory, as in the case of ShinyHunters 2025, which affected Indonesian users, where BSSN led the investigation with data on more than 200 leaks in 2025 (Law Number 27of 2022 on Personal Data Protection, 2022). The relationship with the concept is the principle of aut dedere aut judicare in UN Convention Article 24, which requires countries with perpetrators to extradite or prosecute, as in the 2025 Taiwan attack where Taiwan took the lead but required cooperation with the US to prosecute Chinese actors (Assembly, 2024). For prosecution, PDP Law Article 46 requires rapid reporting, giving Indonesia priority if citizens' personal data is involved, as in the 2025 Telemessage breach case that affected global officials, including potentially in Indonesia (Republic of Indonesia, Law No. 27 of 2022). Normatively, if a conflict occurs, UN Charter Article 2(4) supports coordination through organizations such as INTERPOL, ensuring legal certainty such as the recovery of USD 439 million in 2025 (Arnell & Faturoti, 2023; Schmitt, 2017).

The application of the concept of global legal authority in case studies demonstrates the effectiveness of shared principles for dealing with transnational violations. In the 2025 Taiwan attack, the concept of passive citizenship (victim) from Article 22 of the Budapest Convention was applied, whereby Taiwan led the investigation with evidence of 2.4 million daily attacks, in line with Tallinn Manual Rule 30 on state attribution, resulting in US sanctions against China (Budapest, 2001; Schmitt, 2017). Implications for Indonesia: Similar to the Chinese threat, the KKS Bill could adopt this principle for protective authority, such as in local cases with regional impact (Law Number 27of 2022 on Personal

Data Protection, 2022). In the June 2025 INTERPOL Africa report, the concept of universality from UN Convention Article 40 was applied to ransomware (17,849 cases in South Africa), with global cooperation, factual evidence of a 50% increase since 2024 (Assembly, 2024). Implications: Indonesia can use Article 30 of the ITE Law for similar investigations, strengthening the BSSN with asset recovery data (Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions, 2024). In the September 2025 INTERPOL operation, the concept of jurisdiction was applied to recover USD 439 million, in line with Article 23 of the Budapest Convention, evidence of bilateral cooperation (Budapest, 2001). Implications: The PDP Law can be integrated with the KKS Bill for cyber financial prosecution, increasing legal certainty in ASEAN (Law Number 27of 2022 on Personal Data Protection, 2022). Overall, this application demonstrates the need for Indonesia to ratify the UN Convention, with Global Outlook 2025 data emphasizing fraud as a high risk (Assembly, 2024; Huang, 2024; Pettoello-Mantovani, 2024).

Practical Recommendations

Based on the above analysis and discussion, the following are practical recommendations that can be applied in the context of developing a legal framework and legal certainty in Indonesia.

1. For the development of a legal framework, the Indonesian government is recommended to immediately ratify the UN Convention against Cybercrime after it is opened for signature on October 25, 2025, by integrating its principles into the KKS Bill through amendments that add specific provisions on joint authority and mutual legal assistance, which can be implemented through the legislative process of the Indonesian House of Representatives within one year (United).
2. To enhance legal certainty, the Ministry of Law and Human Rights can develop judicial interpretation guidelines that clarify the definition of crime scenes in the cyber context, based on the Tallinn Manual 2.0, and disseminate them through training for judges and prosecutors, which can be implemented through continuing education programs with a BSSN budget of Rp500 billion per year (Schmitt, 2017).
3. The establishment of a national inter-agency task force, involving the National Cyber and Encryption Agency (BSSN), the Indonesian National Police (Polri), and the Ministry of Foreign Affairs, for the coordination of transnational investigations, with standard protocols in line with Articles 23-35 of the Budapest Convention, can be implemented through a presidential regulation within six months to handle cases such as INTERPOL (Europe) financial attacks. These recommendations are designed to be executed in stages, with annual evaluations to ensure effectiveness and adaptation to new threats.
4. For law enforcement, BSSN and Polri are recommended to implement annual digital forensics training for officers dealing with cybercrime, focusing on locus delicti attribution using tools such as log analysis, in line with UNODC recommendations to combat AI-based cybercrime in Indonesia. In addition, a special unit should be formed within the Attorney General's Office for cases of joint jurisdiction, such as cooperation with ASEANPOL for the extradition of transnational fraudsters, with a target of resolving 50% of cases within 6 months. Annual evaluations through independent audits should be conducted to ensure compliance with the PDP Law and reduce cybercrime losses by 30% by 2026.

The recommendations also cover key challenges in aligning Indonesian telecommunications law with international conventions, including potential conflicts between cybersecurity and human rights protection, which can be addressed through the ratification of global conventions and the updating of national regulations to achieve balance (Assembly, 2024; International Commission of Jurists, 2023).

CONCLUSION

This study concludes that determining jurisdiction and the scene of the crime in transnational cybercrime requires a joint approach based on global legal principles, whereby the scene of the crime is not limited to a single physical location but also includes virtual elements and impacts. Indonesia, through the ITE Law, PDP Law, and KKS Bill, already has a strong national foundation, but ratification of the Budapest Convention and the 2024 UN Convention will increase the effectiveness of international cooperation, reduce conflicts of jurisdiction, and strengthen law enforcement against attacks such as data extortion and espionage. The main recommendation is to align national regulations with global standards to protect the interests of the state in the digital age (Assembly, 2024; Budapest, 2001).

This study contributes to the development of law in Indonesia by strengthening the role of the state as an active actor in global cybercrime, where Indonesia is still limited as an ASEAN member that is often the target of transnational fraud. By adapting the concept of international authority to the

domestic context, this study supports the strengthening of the KKS Bill to improve the resilience of critical infrastructure, reduce economic losses from cybercrime, which are estimated to reach Rp 29.7 billion by 2025 (BSSN data), and position Indonesia as a regional leader in cyber law harmonization, in line with UNODC recommendations for cooperation against the exploitation of AI in cybercrime in Southeast Asia.

REFERENCES

Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, *37*(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888

Assembly, U. N. G. (2024). *United Nations Convention against Cybercrime*.

Budapest. (2001). *Convention on Cybercrime*. Council of Europe.

Colangelo, A. J. (2009). Universal Jurisdiction As An International "False Conflict" of Laws. *Michigan Journal of International Law*, *30*, 881–925. https://doi.org/10.1017/aju.2019.49

Crime, U. N. O. on D. and. (2025). *Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia*.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Fachri, F. K. (2022, November 3). Perkembangan Pembahasan Konvensi Kejahatan Siber di PBB. *Hukum Online.Com*. https://www.hukumonline.com/berita/a/perkembangan-pembahasan-konvensi-kejahatan-siber-di-pbb-lt6362ae18adfe5/

Galih, Y. S. (2019). Yurisdiksi Hukum Pidana Dalam Dunia Maya. *Jurnal Ilmiah Galuh Justisi*, *7*(1), 59. https://doi.org/10.25157/jigj.v7i1.2138

Huang, Z. (2024). Exploring the Territorial Jurisdiction of Cybercrime in the ICC: An Application of the Doctrine of "Effects." *Transactions on Social Science, Education and Humanities Research*, *12*, 15–21. https://doi.org/10.62051/61e72q59

Ibold, V. (2020). Transnational Jurisdiction for Cybercrimes de lege lata and de lege ferenda. *European Criminal Law Review*, *10*(3), 255–271. https://doi.org/10.5771/2193-5505-2020-3-255

Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, 25 (2008).

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pub. L. No. LN.2022/No.196, TLN No.6820, jdih.setneg.go.id, 34 (2022).

Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, (2024).

International Commission of Jurists. (2023). *Indonesia: Newly revised ITE Law threatens freedom of expression and must be amended*. icj.org.

Maillart, J.-B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum*, *19*(3), 375–390. https://doi.org/10.1007/s12027-018-0527-2

Marzuki, P. M. (2019). *Penelitian Hukum Edisi Revisi* (11th ed.). Kencana Prenada Media Group.

Nugroho, A., & Chandrawulan, A. A. (2023). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, *36*(4), 651–670. https://doi.org/10.1057/s41284-022-00357-y

Nyoto. (2021). Perception of PGSD FKIP UPR Students on the Independent Campus Learning Program. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *4*(4), 13515–13520.

Pakaya, R. D., & Mahyani, A. (2022). Landasan Perumusan Locus Delicti Dalam Surat Dakwaan Pada Kejahatan Siber. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, *2*(1), 673–686. https://doi.org/10.53363/bureau.v2i1.160

Permana, R. H. (2025). 110 WNI Kabur dari Bisnis Online Scam Kamboja, 67 Orang Segera Dipulangkan. *Detiknews*. https://news.detik.com/berita/d-8173321/110-wni-kabur-dari-bisnis-online-scam-kamboja-67-orang-segera-dipulangkan

Pettoello-Mantovani, C. (2024). Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction. *International Journal of Law and Politics Studies*, *6*(2), 06–11. https://doi.org/10.32996/ijlps.2024.6.2.2

Prakasa, P. A. (2024). Polisi Ungkap Kasus Pencurian Data Kartu Kredit, Kerugian Miliaran Rupiah. *Medcom.Id*. https://www.medcom.id/nasional/daerah/zNAQo7ZN-polisi-ungkap-kasus-pencurian-data-kartu-kredit-kerugian-miliaran-rupiah

Purwaningsih, R., & Putranto, R. D. (2023). Tinjauan Yuridis Terhadap Penetapan Locus Delicti dalam

Kejahatan Dunia Maya (Cyber Crime) Berkaitan Dengan Upaya Pembaharuan Hukum Pidana di Indonesia. *Mimbar Keadilan*, *16*(1), 130–138. https://doi.org/10.30996/mk.v16i1.8021

Putri Ramli A. F., N. W. "E-Court Dan E-Litigation: Refleksi Atas Digitalisasi Layanan Pengadilan Di Indonesia." *Jurnal Peradilan Digital*, vol. 4, no. 1, 2021, pp. 77–95

Rusydi, M. T. (2025). Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats. *Journal of Progressive Law and Legal Studies*, *3*(01), 69–85. https://doi.org/10.59653/jplls.v3i01.1365

Ryngaert, C. (2025). The Concept of Jurisdiction in International Law. In *Research Hanbook on Jurisdiction and Immunities in International Law* (pp. 37–51). Elgaronline. https://doi.org/https://doi.org/10.4337/9781035331086.00007

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Tzouvala, N. (2015). TWAIL and the "Unwilling or Unable" Doctrine: Continuities and Ruptures. *AJIL Unbound*, *109*, 266–270. https://doi.org/10.1017/S2398772300001574

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.

Widiastuti, A., & Saragih, Y. M. (2025). Transnational Cyber Crime: Challenges of International Cooperation in Combating Cybercrime. *International Journal of Contemporary Sciences*, *2*(9), 999–1012. https://doi.org/https://doi.org/10.55927/ijcs.v2i9.132