IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

Law Enforcement Against Transnational Cybercrime:Jurisdictional Problems and Regulatory Harmonization

Rahmatilah
Dosen UIN Alauddin Makassa, Indonesia

Received: April 03, 2026
Revised: May 05, 2026
Accepted: May 20, 2026
Published: May 30, 2026

Corresponding Author:
Author Name*: Rahmatilah
E-mail*: rahmatiah@uin-alauddin.ac.id

Abstract: *The rapid development of information and communication technology has given rise to the phenomenon of transnational cybercrime, which challenges conventional criminal law, particularly the doctrine of territorial jurisdiction. This article aims to critically analyze the jurisdictional issues in law enforcement against transnational cybercrime and the urgency of regulatory harmonization at the global and regional levels. Using normative legal research methods based on statute, comparative, and conceptual approaches, this study finds that jurisdictional conflicts between countries constitute a structural obstacle stemming from the incompatibility between the concept of territorial state sovereignty and the borderless nature of cybercrime. Furthermore, harmonization efforts through the Budapest Convention have not achieved universal acceptability due to resistance from developing countries that view it as a Western instrument. Indonesia, as a country with high internet penetration, faces a dual challenge: limited domestic regulations and the absence of ratification of relevant international legal instruments. This study concludes that effective law enforcement against transnational cybercrime necessitates reform of international criminal law through an inclusive multilateral approach, strengthening of mutual legal assistance mechanisms, and transforming the jurisdictional paradigm from the principle of territoriality to the contextual effects doctrine principle.*

Keywords: Transnational Cybercrime; Jurisdiction; Regulatory Harmonization; Budapest Convention; International Criminal Law.

INTRODUCTION

The digital transformation that has accelerated since the end of the 20th century has fundamentally altered patterns of human interaction, the structure of the global economy, and the architecture of security threats worldwide. The internet, as the technological infrastructure that forms the backbone of contemporary civilization, has not only opened new horizons for progress but also given rise to a criminal ecosystem previously unimaginable within conventional criminal law. According to the Global Cybersecurity Index

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

report published by the International Telecommunication Union (ITU), global losses from cybercrime are estimated to exceed the international narcotics trade.[1]

Transnational cybercrime is a category of crime that has two simultaneous dimensions: first, a technical dimension that reflects the inherent characteristics of cyberspace as a medium without physical boundaries (borderless cyberspace); and second, a legal dimension that reflects the tension between the concept of state sovereignty that is based on the principle of territoriality and the phenomenon of crime that naturally transcends the boundaries of national jurisdiction.[2]Crimes such as electronic fraud, unauthorized access to information systems, malware distribution, massive personal data theft, and cyberattacks on critical state infrastructure can all be committed from anywhere in the world, with victims spread across multiple jurisdictions.[3]

International criminal law has historically been built on the principle of territoriality, which assumes that states have exclusive authority to regulate and punish acts occurring within their territory. This principle faces fundamental epistemological challenges when dealing with cybercrime, where the perpetrators, victims, the infrastructure used (servers, routers, communication lines), and the consequences of the crime can all be located simultaneously in different countries.[4] The question of which country has the authority to conduct investigations, prosecutions and sentencing becomes a jurisdictional dispute that often results in a jurisdictional vacuum, a situation where no country effectively carries out its law enforcement functions.[5]

From a public international law perspective, jurisdictional issues in transnational cybercrime directly intersect with fundamental principles such as non-interference, sovereign equality, and the due diligence obligation of states to prevent the use of their territory as a base for illegal activities against other states.[6] Indonesia, as the world's fourth-largest internet user, faces increasingly complex challenges. Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendment through Law No. 19 of 2016 have indeed implemented the principle of extraterritorial jurisdiction in Article 2, but its implementation in cross-border cases still leaves serious problems.[7]

Obstacles to law enforcement against transnational cybercrime lie not only in differences in legal systems between countries, but also in disparities in the institutional and technological capacity of law enforcement agencies in conducting digital investigations. In practice, the process of tracking cybercriminals is often

[1]International Telecommunication Union (ITU), "Global Cybersecurity Index 2022", Geneva: ITU, 2023, hlm. 4.

[2]UNODC, "Cybercrime Module 1: Introduction to Cybercrime", E4J University Module Series: Cybercrime, Vienna: UNODC, 2019, hlm. 3.

[3]Susan W. Brenner, "Cybercrime: Criminal Threats from Cyberspace", Santa Barbara: Praeger, 2010, hlm. 12.

[4]Council of Europe, "Convention on Cybercrime (Budapest Convention)", ETS No. 185, Budapest, 23 November 2001, pembukaan.

[5]Didik Endro Purwoleksono, "Hukum Pidana", Surabaya: Airlangga University Press, 2014, hlm. 25–27.

[6]Antonio Cassese, "International Criminal Law", 2nd ed., Oxford: Oxford University Press, 2008, hlm. 335.

[7]Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang No. 19 Tahun 2016, Pasal 2.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

hampered by the use of anonymization technologies such as Virtual Private Networks (VPNs), end-to-end encryption, the dark web, and spoofing techniques, which make it difficult to identify the locus delicti and the perpetrator's identity.[8] This situation makes electronic evidence highly vulnerable to jurisdictional and procedural validity disputes, particularly when the digital data resides on servers located in other countries and is subject to different data protection regimes. The issue becomes even more complex when the country where the data resides refuses access, citing concerns about digital sovereignty or the privacy rights of its citizens.[9] As a result, the mutual legal assistance (MLA) mechanism, which has been the primary instrument for international criminal cooperation, is deemed no longer adequate to meet the needs of cyber law enforcement, which demands fast data access and real-time responses to dynamic digital threats.

Beyond technical and procedural issues, global regulatory fragmentation also demonstrates the differing paradigms among countries regarding cyberspace governance. Developed nations tend to position cybersecurity as part of national security interests and digital economic stability, while many developing countries still face limitations in regulations, infrastructure, and human resources to build effective cybersecurity regimes.[10] These differing orientations have given rise to disharmonious legal norms, including those concerning the definition of cybercrime, standards for electronic evidence, extradition mechanisms, and the limits of state authority in conducting cross-border cybersurveillance. The absence of universal international legal standards often results in partial and unilateral law enforcement against cybercrime.[11] In fact, the transnational nature of cybercrime demands a collective approach based on regulatory harmonization, interoperability of legal systems, and strengthening international cooperation to prevent the creation of safe havens for digital criminals in countries with weak regulations or those not yet integrated with the international cyber law regime.[12]

Various regulatory harmonization efforts have been undertaken, ranging from the Budapest Convention on Cybercrime (2001), the first international legal instrument to comprehensively regulate cybercrime, to regional initiatives such as the ASEAN Cybersecurity Cooperation Framework. However, the effectiveness of these instruments remains questionable, particularly given the Budapest Convention's low acceptance among developing countries, which consider its drafting process to be non-inclusive and its substance too

[8] Wibowo, Muhammad Singgih Imam, and Akhmad Munawar. "Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia." *Jurnal Hukum Lex Generalis* 5.7 (2024). https://rewangrencang.com/ojs/index.php/JHLG/article/view/641

[9] Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 13.2 (2023): 222-238. http://dx.doi.org/10.22212/jp.v13i2.3299

[10] Ulwan, Abdurrahman Nashih Wildan. "Strategi Politik Luar Negeri Indonesia dalam Menghadapi Ancaman Siber Transnasional: Analisis Diplomasi Siber dan Kerja Sama Internasional." *Indonesian Journal of Humanities and Social Sciences* 7.1 (2026): 197-214. https://doi.org/10.33367/ijhass.v7i1.9049

[11] Himawan, Budi. "Kajian Normatif terhadap Tantangan Penegakan Hukum atas Tindak Pidana Scam Lintas Negara di Era Globalisasi." *Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial, dan Hukum (SENPISHUM)*. Vol. 1. No. 1. 2026. https://journal.unj.ac.id/unj/index.php/senpishum/article/view/62473

[12] Anwar, Syaiful, and Johan Edi Nepri. "Harmonisasi Hukum Digital: Tantangan Global dan Strategi Adaptif Indonesia dalam Era Kedaulatan Siber." *Hutanasyah: Jurnal Hukum Tata Negara* 4.1 (2025): 69-88. https://doi.org/10.37092/hutanasyah.v4i1.1297

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

oriented toward the interests of Western European countries.[13] Based on this background, this article poses two research questions that become the focus of the study: first, how are the jurisdictional problems in law enforcement against transnational cybercrime viewed from the perspective of international criminal law?; and second, what is the urgency and mechanism for harmonizing cybercrime regulations at the global and regional levels in overcoming the limitations of a unilateral approach?[14]

METHODOLOGY

This research is a normative legal research that focuses on doctrinal analysis of positive legal norms, legal principles, and doctrines relevant to the problem under study. In the legal tradition, normative research rests on the premise that law is a system of norms that can be studied autonomously through logical-deductive analysis. The research approach used is triangulative, namely combining three approaches synergistically: First, the statute approach that involves a systematic review of national laws and regulations related to cybercrime, especially the ITE Law, the Criminal Code, Law No. 2 of 2002 concerning the Indonesian National Police, and Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure and international legal instruments such as the Budapest Convention, the UN Convention against Transnational Organized Crime (UNTOC), and various bilateral mutual legal assistance agreements that have been ratified by Indonesia. Second, a comparative approach that compares the legal frameworks of several representative jurisdictions, including the United States (Computer Fraud and Abuse Act), the European Union (Directive on Attacks Against Information Systems 2013/40/EU), Malaysia (Computer Crimes Act 1997), and Singapore (Computer Misuse Act), in order to identify patterns of regulatory convergence and divergence that are relevant for legal reform in Indonesia.

The conceptual approach, which places the analysis at the theoretical and doctrinal level, encompasses the theory of state sovereignty (Bodin, Jellinek), the doctrine of jurisdiction in international law (territorial principle, nationality principle, passive personality principle, protective principle, universality principle), the theory of effects doctrine as developed in United States jurisprudence, and the concept of legal harmonization within a comparative law framework. Primary legal materials include international treaties, national legislation of various countries, relevant jurisprudence of international and national courts, and soft law instruments such as UN General Assembly resolutions and UNODC guidelines. Secondary legal materials include scientific monographs, peer-reviewed articles in international and national law journals, reports from leading research institutions, and official commentaries on international legal instruments. The analysis is conducted qualitatively using grammatical, systematic, teleological, and comparative interpretation techniques.

RESULTS AND DISCUSSION

Jurisdictional Issues in Enforcing Transnational Cybercrime Laws

Jurisdiction in international law refers to a state's authority to regulate, enforce, and adjudicate a particular legal event or subject. Malcolm N. Shaw classifies jurisdiction into three fundamental categories: prescriptive/legislative jurisdiction, which is the authority to create binding legal norms; adjudicative jurisdiction, which is the authority to apply the law through judicial mechanisms; and enforcement

[13]Satjipto Rahardjo, "Ilmu Hukum", Bandung: Citra Aditya Bakti, 2012, hlm. 177.

[14]Mireille Hildebrandt, "Smart Technologies and the End(s) of Law", Cheltenham: Edward Elgar Publishing, 2016, hlm. 56–58.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

jurisdiction, which is the authority to enforce compliance with the law.[15][16]In the historical development of international law, the principle of territorial jurisdiction has been a dominant focal point. The Permanent Court of International Justice's (PCIJ) decision in the Lotus Case of 1927 affirmed that a state has full authority over all events occurring within its territory, but cannot unilaterally extend its jurisdiction to the territory of another state without a strong basis in international law.[17] This principle, although it has historically served as a stabilizer of interstate relations, has proven inadequate to address cybercrime, which is structurally transnational in nature.[18]

The unique characteristics of cyberspace, namely the anonymity of actors, the instantaneousness of data transmission, the ease of encryption, and the multi-configuration of connection points that transcend geographical boundaries, create what Jack Goldsmith and Tim Wu call the "illusion of a borderless world," where conventional law appears paralyzed in the face of the new virtual reality.[19] However, Goldsmith and Wu also argue that nation-states actually still have the capacity to control the internet through regulation of physical entities within their jurisdiction, an argument that implicitly encourages an effects-based jurisdiction approach.[20] The doctrine of jurisdiction in international criminal law recognizes several principles that can be applied cumulatively or alternatively: (1) The territoriality principle in its two variants: subjective territoriality which gives jurisdiction to the country where the crime began, and objective territoriality which gives jurisdiction to the country where the consequences of the crime are felt; (2) The active nationality principle which bases jurisdiction on the nationality of the perpetrator; (3) The passive personality principle which bases jurisdiction on the nationality of the victim; (4) The protective principle which grants jurisdiction based on the vital interests of the country that are threatened; and (5) The universality principle which grants jurisdiction to all countries over crimes that are seen as hostes humani generis. [21][22]

The fundamental paradox of law enforcement against transnational cybercrime lies in the fact that almost all existing jurisdictional principles can be simultaneously claimed by more than one country for the same crime, or conversely—no country feels it has sufficient jurisdiction to take action. Indonesia's ITE Law, as reflected in Article 2, adopts an extraterritorial approach by stating that the ITE Law applies to anyone who commits a legal act as regulated in this Law, whether within or outside Indonesia.[23] This type of extraterritorial formulation, while reflecting the legislators' desire to keep pace with developments in international law, poses a number of serious implementation issues. Claims of extraterritorial jurisdiction

[15]Council of Europe, "Explanatory Report to the Convention on Cybercrime", Budapest Convention, ETS No. 185, 2001, para. 22.

[16]Malcolm N. Shaw, "International Law", 8th ed., Cambridge: Cambridge University Press, 2017, hlm. 486–490.

[17]Lotus Case (France v. Turkey), Permanent Court of International Justice, 1927, PCIJ Series A No. 10.

[18]Brigitte Stern, "The Elements of an Internationally Wrongful Act" dalam James Crawford (ed.), "The Law of International Responsibility", Oxford: Oxford University Press, 2010, hlm. 193–194.

[19]Jack Goldsmith & Tim Wu, "Who Controls the Internet? Illusions of a Borderless World", New York: Oxford University Press, 2006, hlm. 67–69.

[20]Sieber Ulrich, "Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law" dalam M. Delmas-Marty et al. (eds.), "Harmonising Criminal Law", Paris: Société de Législation Comparée, 2008, hlm. 195–196.

[21]Danielle Citron, "Hate Crimes in Cyberspace", Cambridge: Harvard University Press, 2014, hlm. 221–224.

[22]Amos N. Guiora, "Cybersecurity: Geopolitics, Law, and Policy", New York: Routledge, 2017, hlm. 45–47.

[23]Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang No. 19 Tahun 2016, Penjelasan Pasal 2.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

without adequate bilateral treaty support would be merely symbolic norms with no real enforcement power, as other countries have no legal obligation to extradite perpetrators or hand over digital evidence.[24]

Positive jurisdictional conflict—a situation in which more than one country claims jurisdiction over the same case—can give rise to the problem of ne bis in idem at the international level, which has not yet been satisfactorily resolved in positive international law. Eddy OS Hiariej notes that the principle of ne bis in idem in the international context remains controversial because it is not universally recognized as a ius cogens norm, so a cybercriminal could theoretically be prosecuted repeatedly in different countries for the same act.[25] The problem of negative jurisdictional conflict, or jurisdictional vacuum, occurs when none of the countries involved feels they have sufficient jurisdiction—or sufficient political interest—to take legal action. A 2022 Interpol report revealed that most transnational cybercrime syndicates operating globally choose to base themselves in countries with weak cyber regulations or ineffective law enforcement, exploiting these jurisdictions as safe havens for their criminal activities.[26]

Shinya Watanabe's comparative study of cybercrime jurisprudence in the United States, the European Union, and several Asian countries shows that even countries with relatively developed legal frameworks still struggle to effectively enforce their jurisdiction in complex cross-border cases, especially when digital evidence is stored on servers located in uncooperative jurisdictions.[27] One of the most pressing points of tension in transnational cybercrime law enforcement is the antinomy between the demands of effective law enforcement and respect for the territorial sovereignty of other states. Cross-border investigative actions conducted without the consent of the state concerned—such as remote access to servers located outside national jurisdiction (trans-border search and seizure)—have traditionally been viewed as violations of sovereignty that can give rise to state responsibility under international law.[28]

Peter Grabosky identifies that the absence of a general international legal obligation to provide assistance in criminal law enforcement is a very significant lacuna in the international legal architecture.[29] Existing Mutual Legal Assistance Treaties (MLATs) are unable to keep up with the speed of digital transactions; conventional mutual legal assistance requests can take months to process, while digital evidence can be deleted, encrypted, or transferred in seconds. At the regional level, the ASEAN Cybersecurity Cooperation Strategy 2021–2025 offers a more adaptive framework, but it remains voluntary and non-legally binding.[30] The absence of a mandatory enforcement mechanism makes this regional strategy vulnerable to the free-rider problem, where countries with weak cyber governance benefit from cooperation without bearing the

[24]Yudha Bhakti Ardhiwisastra, "Imunitas Kedaulatan Negara di Forum Pengadilan Asing", Bandung: Alumni, 1999, hlm. 42.

[25]Eddy O.S. Hiariej, "Prinsip-Prinsip Hukum Pidana", Yogyakarta: Cahaya Atma Pustaka, 2016, hlm. 68–70.

[26]Interpol, "2022 Cyberthreat Assessment", Lyon: Interpol Cybercrime Directorate, 2022, hlm. 11.

[27]Shinya Watanabe, "Territoriality and Internet Jurisdiction: Comparative Perspectives on Cybercrime Law", Journal of International Criminal Justice, Vol. 18, No. 3, 2020, hlm. 605–627.

[28]Hazel Glenn Beh, "The Performance of Death: Uncovering Prosecutorial Discretion under the Federal Death Penalty Act", University of Illinois Law Review, 1999, hlm. 113.

[29]Peter Grabosky, "Cybercrime: The Challenge in Asia", dalam Roderic Broadhurst & Peter Grabosky (eds.), "Cybercrime: The Challenge in Asia", Hong Kong: Hong Kong University Press, 2005, hlm. 7–9.

[30]ASEAN, "ASEAN Cybersecurity Cooperation Strategy 2021–2025", Jakarta: ASEAN Secretariat, 2021, hlm. 6.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

burden of equal obligations. This is further exacerbated by disparities in technical capacity and law enforcement resources among the highly heterogeneous ASEAN member states.[31]

From a legal theory perspective, this jurisdictional problem essentially reflects a paradigmatic crisis in international criminal law, which has yet to adapt to the fundamental changes brought about by digitalization. As criticized by Debarati Halder, international criminal law remains too tied to the Websterian assumption of the state as the primary actor in the international legal system, even though cybercrime often involves non-state actors such as hacktivist groups, organized cybercrime syndicates, and even solitary individuals who cannot be reduced to conventional state-centric analytical frameworks.[32]

Harmonization of Cybercrime Regulations: An Unfinished Global Agenda

The Budapest Convention on Cybercrime, adopted by the Council of Europe on 23 November 2001 and entered into force on 1 July 2004, is the first international treaty to systematically seek to harmonize substantive and procedural cybercrime law between States.[33] As of May 2026, the convention has been ratified by more than 60 countries, including several countries outside Europe such as the United States, Japan, and Australia, indicating its relevance beyond the European regional context in which it was born.[34] Substantively, the Budapest Convention regulates four main categorizations of cybercrime: (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offenses; (3) content-related offenses; and (4) offenses related to infringements of copyright and related rights. In addition, this convention also regulates procedural provisions such as expedited preservation of stored computer data, disclosure of preserved traffic data, production orders, search and seizure, real-time collection of traffic data, and interception of content data.[35]

From a legal harmonization perspective, the Budapest Convention has been praised for providing a common reference point for countries developing or reforming their cyber legal frameworks. Marc D. Goodman and Susan W. Brenner note that the convention has contributed significantly to establishing a minimum consensus on the types of conduct that member states should criminalize, although considerable room for national discretion remains.[36] However, the Budapest Convention faces fundamental criticism, especially from developing countries.[37] First, there's a critique of the process: non-European countries were not

[31]Debarati Halder & K. Jaishankar, "Cyber Crime and the Victimization of Women: Laws, Rights and Regulations", Hershey: IGI Global, 2012, hlm. 84.

[32]Council of Europe, "T-CY Guidance Note #3: Transborder Access to Data (Article 32)", Cybercrime Convention Committee, 2013, para. 9.

[33] Spiezia, Filippo. "International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime." *ERA Forum*. Vol. 23. No. 1. Berlin/Heidelberg: Springer Berlin Heidelberg, 2022. https://doi.org/10.1007/s12027-022-00707-8

[34]Ardi Ferdian, "Konstruksi Hukum Tindak Pidana Siber Lintas Batas dalam Perspektif Hukum Internasional", Jurnal Hukum & Pembangunan, Vol. 51, No. 2, 2021, hlm. 312–330.

[35]Wahyudi Djafar, "Perlindungan Data Pribadi dalam Sistem Hukum Nasional: Antara Kebutuhan dan Tantangan Implementasi", Jurnal HAM, Vol. 13, No. 1, 2022, hlm. 55–74.

[36]United Nations General Assembly, "Report of the Open-ended Intergovernmental Expert Group on Cybercrime", A/AC.287/2021/CRP.4, Vienna: UNODC, 2021.

[37] Apsimet, N. M., and A. Zh Muratova. "On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud." *Bulletin of the Karaganda University "Law Series"* 11730.1 (2025): 87-97. https://doi.org/10.31489/2025l1/87-97

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

involved in the negotiation and formulation of this convention, so its substance reflects the perspectives and interests of Western countries that already have a more established legal and technical infrastructure. Hikmahanto Juwana, an Indonesian international law expert, emphasizes that the legitimacy of an international legal instrument in a post-colonial context depends heavily on the inclusiveness of its drafting process.[3839]

Second, substantive criticism of Article 32(b) of the Budapest Convention, which permits trans-border access to data stored on servers in other countries without prior permission, as long as the data is "lawfully accessible from the public" or with the consent of the data owner. This provision is viewed by Russia, China, and a number of developing countries as legalizing actions that potentially violate their digital sovereignty—a form of cyber imperialism disguised in the language of law enforcement.[40] Third, the capacity critique: The Budapest Convention assumes the availability of legal and technical infrastructure that developing countries do not necessarily possess. The obligation to provide a 24/7 network of contact points, implement expedited preservation procedures, and conduct real-time collection of traffic data requires significant institutional and technological investment—which in many cases exceeds the fiscal and technical capacities of developing countries.[41]

At the regional level in Southeast Asia, efforts to harmonize cybercrime regulations are taking place within a more fragmented framework. ASEAN has adopted several instruments, such as the ASEAN Agreement on Electronic Commerce (2019) and the ASEAN Cybersecurity Cooperation Strategy, but these instruments focus more on cybersecurity aspects than on cybercrime in the criminal sense. The absence of an ASEAN legal instrument specifically regulating the harmonization of cybercriminal law—analogous to the Budapest Convention in Europe—represents a significant normative gap.[42] A comparative study of the legal frameworks of ASEAN countries reveals stark regulatory disparities. Singapore, with its Computer Misuse Act (1993, last revised in 2017), and Malaysia, with its Computer Crimes Act (1997), have relatively comprehensive legal frameworks that have undergone several updates. In contrast, several other ASEAN countries still rely on general criminal law provisions that are simply not designed to address the complexities of cybercrime.[43]

Indonesia itself faces multi-layered challenges. At the substantive regulatory level, the ITE Law—despite its 2016 revision and ongoing debate over a second revision—still contains several fundamental weaknesses. The articles governing specific cybercrimes remain partial and do not comprehensively cover the evolving typology of cybercrimes, such as ransomware, cryptojacking, deepfake-mediated fraud, and

[38]Assafa Endeshaw, "Internet Regulation in Asia", Singapore Journal of Legal Studies, 2004, hlm. 105–131.

[39]Marc D. Goodman & Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", International Journal of Law and Information Technology, Vol. 10, No. 2, 2002, hlm. 139–223.

[40]Hikmahanto Juwana, "Hukum Internasional dalam Perspektif Indonesia sebagai Negara Berkembang", Jakarta: Yarsif Watampone, 2010, hlm. 38.

[41]Romli Atmasasmita, "Hukum Pidana Internasional dalam Kerangka Perdamaian dan Keamanan Internasional", Bandung: Fikahati Aneska, 2010, hlm. 122–125.

[42]Insa Neumann, "The UN Cybercrime Convention: Will a Global Treaty Help or Hinder the Fight against Cybercrime?", Journal of International Law and International Relations, Vol. 19, 2023, hlm. 1–29.

[43]Monika Zalnieriute & Lyria Bennett Moses, "The Rule of Law and Technology" dalam Jacques deLisle & Avery Goldstein (eds.), "To Govern the Globe: World Orders and Catastrophic Change", Stanford: Stanford University Press, 2021, hlm. 317.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

attacks on IoT-based critical infrastructure.[44] More critically, Indonesia has not yet ratified the Budapest Convention and lacks a clear policy on whether to join it. This ambiguity places Indonesia in an ambiguous position: too large and too exposed to cybercrime risks to ignore international instruments, yet also having legitimate objections to the substance of the convention, which it deems inadequately accommodates the interests of developing countries.[45]

At the procedural level, Indonesia's mutual legal assistance mechanism rests on Law No. 1 of 2006 concerning Mutual Assistance in Criminal Matters. While this framework provides the necessary legal basis, its implementation in cybercrime cases faces serious practical obstacles: the procedures are too bureaucratic and slow to keep pace with the speed of digital transactions, the coverage of treaty partner countries remains limited, and the capacity of cyber law enforcement units remains uneven.[46] One positive development worth noting is the establishment of the National Cyber and Crypto Agency (BSSN) through Presidential Regulation No. 28 of 2021, which consolidates national cybersecurity functions. However, the BSSN's mandate, which focuses more on cyber defense than on criminal law enforcement, creates institutional silos that could hamper a unified response to transnational cybercrime.[47]

The negotiation process for a universal UN Convention on Cybercrime, initiated by UN General Assembly Resolution A/RES/74/247 in 2019, represents the most ambitious effort to build a global consensus. Insa Neumann notes that the negotiations for the UN convention are essentially a battle between two coalitions: Western countries, which want to minimize duplication with the Budapest Convention and maintain a focus on law enforcement, versus Russia, China, and a number of developing countries, which want broader coverage, including cyber sovereignty and counter-terrorism.[48] From a comparative law perspective, regulatory harmonization does not mean total legal uniformity, but can operate at several different levels: principle-level harmonization, minimum harmonization, or substantial harmonization. In the context of transnational cybercrime, a minimum harmonization approach that establishes a floor of protection without eliminating state discretion to apply higher standards appears to be the most politically realistic.[49]

The Carnegie Endowment for International Peace recommends that an effective global cyber convention should meet three essential criteria: (1) inclusiveness of the process—involving all stakeholders including developing countries, civil society, and the private sector; (2) balance of values—balancing the need for law enforcement with the protection of human rights and digital privacy; and (3) adaptability—having a mechanism for regular updates that allows the convention to keep pace with technological developments.[50] For Indonesia specifically, Wahyudi Djafar argues that strengthening domestic law enforcement capacity

[44]Cyber Policy Initiative, "Toward a Global Convention on Cybercrime: The Budapest Convention and Beyond", Carnegie Endowment for International Peace, Policy Brief, 2020, hlm. 5.

[45]Edmon Makarim, "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik", Jakarta: RajaGrafindo Persada, 2010, hlm. 78.

[46]Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital, Pasal 5.

[47]Tobias Mahler, "Generic Top-Level Domains: A Study of Transnational Private Governance", Alphen aan den Rijn: Kluwer Law International, 2019, hlm. 203–204.

[48]Ryan Goodman & Derek Jinks, "Socializing States: Promoting Human Rights through International Law", Oxford: Oxford University Press, 2013, hlm. 11–13.

[49]UNODC, "Comprehensive Study on Cybercrime", Draft February 2013, New York: United Nations, 2013, hlm. xx–xxi.

[50]Cyber Policy Initiative, "Toward a Global Convention on Cybercrime: The Budapest Convention and Beyond", Carnegie Endowment for International Peace, Policy Brief, 2020, hlm. 6.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

must run parallel to active diplomatic engagement in the formation of international cyber norms.[51] Without adequate domestic capacity, Indonesia will always be in a reactive position—following standards set by dominant actors without being able to influence the formation of those norms. Conversely, without active engagement in international forums, Indonesia's interests—especially those related to protecting digital sovereignty and internet users' rights—risk being neglected.[52]

A multilevel governance approach also needs to be considered as an alternative analytical framework. Tobias Mahler argues that effective cyber governance cannot rely solely on state-centric legal instruments, but rather requires the integration of non-state actors—particularly technology platform companies, internet service providers, and the cybersecurity research community—into a more complex regulatory ecosystem.[53] Models of co-regulation and self-regulation combined with strong public oversight offer the potential to fill regulatory gaps that cannot be addressed solely through traditional international legal instruments.[54] Overall, effective harmonization of transnational cybercrime regulations necessitates a paradigmatic transformation in how states view the relationship between sovereignty and digital interdependence. Digital sovereignty in the internet era can no longer be understood as a state's exclusive and absolute right to cyberspace operating on its infrastructure, but rather as responsible sovereignty, which requires the fulfillment of due diligence obligations to prevent a state's cyberspace from becoming a base for crimes against other states—as has begun to be recognized in the Tallinn Manual on the International Law Applicable to Cyber Operations.[55]

CONCLUSIONS

The jurisdictional problem in law enforcement against transnational cybercrime stems from the structural incompatibility between the Westphalian paradigm of territorial state sovereignty and the inherent borderless nature of cyberspace. Jurisdictional conflicts—both positive and negative—constitute a systemic obstacle that cannot be overcome unilaterally, and a unilateral extraterritorial approach such as that adopted by Indonesia in Article 2 of the ITE Law will remain merely a symbolic norm without real enforcement power unless supported by adequate bilateral or multilateral agreements. Second, efforts to harmonize regulations through the Budapest Convention, while a significant normative achievement, face difficult-to-overcome political and epistemological limitations: a legitimacy deficit resulting from a non-inclusive drafting process, provisions that potentially violate the digital sovereignty of developing countries, and a vast gap in implementation capacity among signatory countries. This situation creates an urgent need for a new global instrument born from a genuine and inclusive negotiation process, as is being pursued through the UN framework. Third, Indonesia needs to take a more proactive strategic position in international cyber governance. This includes: comprehensive reform of the ITE Law that broadens the scope of cybercrime typologies while strengthening international cooperation mechanisms; accelerating the technical and institutional capacity of cyber law enforcement agencies; strengthening the MLAT network with key

[51]Wahyudi Djafar, "Perlindungan Data Pribadi dalam Sistem Hukum Nasional: Antara Kebutuhan dan Tantangan Implementasi", Jurnal HAM, Vol. 13, No. 1, 2022, hlm. 68.

[52]Wahyudi Djafar, loc. cit., hlm. 70.

[53]Tobias Mahler, "Generic Top-Level Domains: A Study of Transnational Private Governance", Alphen aan den Rijn: Kluwer Law International, 2019, hlm. 207.

[54]Ryan Goodman & Derek Jinks, "Socializing States: Promoting Human Rights through International Law", Oxford: Oxford University Press, 2013, hlm. 15.

[55]Michael N. Schmitt (ed.), "Tallinn Manual on the International Law Applicable to Cyber Operations", Cambridge: Cambridge University Press, 2013, Rules 1–4.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

partner countries; and active involvement in the UN Convention on Cybercrime negotiation process to ensure the interests of developing countries are accommodated. Finally, from a legal theory perspective, effective law enforcement against transnational cybercrime requires a paradigmatic shift from an absolute digital sovereignty model to a responsible digital sovereignty model that integrates sovereign rights with international due diligence obligations. Without this paradigmatic transformation, international criminal law will continue to lag behind the pace of technological innovation—and cybercrime will continue to thrive in unaddressed jurisdictional gaps.

REFERENCES

Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 13.2 (2023): 222-238. http://dx.doi.org/10.22212/jp.v13i2.3299

Anwar, Syaiful, and Johan Edi Nepri. "Harmonisasi Hukum Digital: Tantangan Global dan Strategi Adaptif Indonesia dalam Era Kedaulatan Siber." *Hutanasyah: Jurnal Hukum Tata Negara* 4.1 (2025): 69-88. https://doi.org/10.37092/hutanasyah.v4i1.1297

Apsimet, N. M., and A. Zh Muratova. "On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud." *Bulletin of the Karaganda University "Law Series"* 11730.1 (2025): 87-97. https://doi.org/10.31489/2025l1/87-97

Ardhiwisastra, Yudha Bhakti. Imunitas Kedaulatan Negara di Forum Pengadilan Asing. Bandung: Alumni, 1999.

ASEAN. ASEAN Cybersecurity Cooperation Strategy 2021–2025. Jakarta: ASEAN Secretariat, 2021.

Assafa Endeshaw. "Internet Regulation in Asia." Singapore Journal of Legal Studies, 2004, hlm. 105–131.

Atmasasmita, Romli. Hukum Pidana Internasional dalam Kerangka Perdamaian dan Keamanan Internasional. Bandung: Fikahati Aneska, 2010.

Brenner, Susan W. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger, 2010.

Cassese, Antonio. International Criminal Law. 2nd ed. Oxford: Oxford University Press, 2008.

Citron, Danielle. Hate Crimes in Cyberspace. Cambridge: Harvard University Press, 2014.

Council of Europe. Convention on Cybercrime (Budapest Convention). ETS No. 185, Budapest, 23 November 2001.

Council of Europe. Explanatory Report to the Convention on Cybercrime. Budapest Convention, ETS No. 185, 2001.

Council of Europe. T-CY Guidance Note #3: Transborder Access to Data (Article 32). Cybercrime Convention Committee, 2013.

Djafar, Wahyudi. "Perlindungan Data Pribadi dalam Sistem Hukum Nasional: Antara Kebutuhan dan Tantangan Implementasi." Jurnal HAM, Vol. 13, No. 1, 2022, hlm. 55–74.

Ferdian, Ardi. "Konstruksi Hukum Tindak Pidana Siber Lintas Batas dalam Perspektif Hukum Internasional." Jurnal Hukum & Pembangunan, Vol. 51, No. 2, 2021, hlm. 312–330.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

Goldsmith, Jack & Tim Wu. Who Controls the Internet? Illusions of a Borderless World. New York: Oxford University Press, 2006.

Goodman, Marc D. & Susan W. Brenner. "The Emerging Consensus on Criminal Conduct in Cyberspace." International Journal of Law and Information Technology, Vol. 10, No. 2, 2002, hlm. 139–223.

Goodman, Ryan & Derek Jinks. Socializing States: Promoting Human Rights through International Law. Oxford: Oxford University Press, 2013.

Guiora, Amos N. Cybersecurity: Geopolitics, Law, and Policy. New York: Routledge, 2017.

Halder, Debarati & K. Jaishankar. Cyber Crime and the Victimization of Women: Laws, Rights and Regulations. Hershey: IGI Global, 2012.

Hiariej, Eddy O.S. Prinsip-Prinsip Hukum Pidana. Yogyakarta: Cahaya Atma Pustaka, 2016.

Hildebrandt, Mireille. Smart Technologies and the End(s) of Law. Cheltenham: Edward Elgar Publishing, 2016.

Himawan, Budi. "Kajian Normatif terhadap Tantangan Penegakan Hukum atas Tindak Pidana Scam Lintas Negara di Era Globalisasi." *Prosiding Seminar Nasional Pendidikan, Ilmu-Ilmu Sosial, dan Hukum (SENPISHUM)*. Vol. 1. No. 1. 2026. https://journal.unj.ac.id/unj/index.php/senpishum/article/view/62473

Indonesia. Peraturan Presiden No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.

Indonesia. Peraturan Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital.

Indonesia. Undang-Undang No. 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana.

Indonesia. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 No. 58.

Indonesia. Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008. Lembaran Negara RI Tahun 2016 No. 251.

International Telecommunication Union (ITU). Global Cybersecurity Index 2022. Geneva: ITU, 2023.

Interpol. 2022 Cyberthreat Assessment. Lyon: Interpol Cybercrime Directorate, 2022.

Juwana, Hikmahanto. Hukum Internasional dalam Perspektif Indonesia sebagai Negara Berkembang. Jakarta: Yarsif Watampone, 2010.

Lotus Case (France v. Turkey). Permanent Court of International Justice, 1927, PCIJ Series A No. 10.

Mahler, Tobias. Generic Top-Level Domains: A Study of Transnational Private Governance. Alphen aan den Rijn: Kluwer Law International, 2019.

Makarim, Edmon. Tanggung Jawab Hukum Penyelenggara Sistem Elektronik. Jakarta: RajaGrafindo Persada, 2010.

Neumann, Insa. "The UN Cybercrime Convention: Will a Global Treaty Help or Hinder the Fight against Cybercrime?" Journal of International Law and International Relations, Vol. 19, 2023, hlm. 1–29.

Purwoleksono, Didik Endro. Hukum Pidana. Surabaya: Airlangga University Press, 2014.

Rahardjo, Satjipto. Ilmu Hukum. Bandung: Citra Aditya Bakti, 2012.

Shaw, Malcolm N. International Law. 8th ed. Cambridge: Cambridge University Press, 2017.

Sieber, Ulrich. "Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law." dalam M. Delmas-Marty et al. (eds.), Harmonising Criminal Law. Paris: Société de Législation Comparée, 2008, hlm. 191–216.

Spiezia, Filippo. "International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime." *ERA Forum*. Vol. 23. No. 1. Berlin/Heidelberg: Springer Berlin Heidelberg, 2022. https://doi.org/10.1007/s12027-022-00707-8

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol 3. No.4, May 2026
DOI : https://doi.org/10.62872/wafdhr93

Ulwan, Abdurrahman Nashih Wildan. "Strategi Politik Luar Negeri Indonesia dalam Menghadapi Ancaman Siber Transnasional: Analisis Diplomasi Siber dan Kerja Sama Internasional." *Indonesian Journal of Humanities and Social Sciences* 7.1 (2026): 197-214. https://doi.org/10.33367/ijhass.v7i1.9049

Uni Eropa. Directive 2013/40/EU on Attacks Against Information Systems.

United Nations General Assembly. Report of the Open-ended Intergovernmental Expert Group on Cybercrime. A/AC.287/2021/CRP.4. Vienna: UNODC, 2021.

United States v. Morris, 928 F.2d 504 (2nd Cir. 1991).

UNODC. Comprehensive Study on Cybercrime. Draft February 2013. New York: United Nations, 2013.

UNODC. Cybercrime Module 1: Introduction to Cybercrime. E4J University Module Series: Cybercrime. Vienna: UNODC, 2019.

Watanabe, Shinya. "Territoriality and Internet Jurisdiction: Comparative Perspectives on Cybercrime Law." Journal of International Criminal Justice, Vol. 18, No. 3, 2020, hlm. 605–627.

Wibowo, Muhammad Singgih Imam, and Akhmad Munawar. "Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia." *Jurnal Hukum Lex Generalis* 5.7 (2024). https://rewangrencang.com/ojs/index.php/JHLG/article/view/641