Vol. 01 /No. 01 /2026

Extradition of Cross-Border Cybercrime Perpetrators: A Comparative Study of Indonesia and Singapore

Amizy Nova Airul Ayunda Kurniawan*[1], Kenneth Sulthon Alafi Al Hallaj[2], Eka Firmansyah[3], Dian Prahara Batubara[4], Ghina Ruqayatul Malihah[5]

[1]Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia, amizynova25@gmail.com

[2]Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia, elaphy07@gmail.com

[3]Universitas Muhammadiyah Palu, Indonesia, ekafirmansyah689@gmail.com

[4]Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia, dianbatubara144@gmail.com

[5]Universitas Islam Negeri Sunan Ampel Surabaya, Indonesia, ghinaruqayatul09@gmail.com

*corresponding author: amizynova25@gmail.com

ABSTRACT: Transnational cybercrime challenges traditional state sovereignty and territorial jurisdiction paradigms underpinning extradition, creating acute enforcement gaps exploited by cybercriminal networks. This study conducts a comparative juridical analysis of cybercrime extradition frameworks in Indonesia and Singapore two ASEAN states with contrasting digital economies, distinct legal traditions, and divergent approaches to international cooperation. Utilizing normative legal research with statute, comparative, and case approaches, this study systematically analyzes primary sources (extradition and cybercrime laws, treaties, multilateral frameworks) and secondary scholarly sources from Sinta/Scopus indexed journals. Results identify three central findings: (1) Indonesia and Singapore maintain distinct legislative architectures, with Singapore operating a more sophisticated, integrated framework under the Computer Misuse Act and Extradition Act, contrasting Indonesia's fragmented approach under the EIT Law (UU ITE) and Law No. 1/1979; (2) the absence of a bilateral extradition treaty creates a structural gap impeding the prosecution of cybercriminals exploiting their geographic and jurisdictional proximity; and (3) alternative cross-border mechanisms, including mutual legal assistance (MLA) and INTERPOL, are insufficient substitutes for a treaty based framework given the volume and sophistication of cyber threats. The study concludes by proposing a bilateral cybercrime extradition treaty framework and specific domestic legal reforms to enhance cross border enforcement effectiveness.

Keywords: *Extradition, Cybercrime, Cross-Border Crime, Mutual Legal Assistance, ASEAN Cooperation*

Received: 2026-May-05
Rev. Req: 2026-May-29
Accepted: 2026-June-22

I. INTRODUCTION

The exponential growth of digital connectivity has created unprecedented opportunities for economic and social development while simultaneously generating a global threat landscape in which cybercriminal actors exploit the borderless character of cyberspace to commit offenses that transcend national jurisdictions with minimal risk of effective legal accountability (Siswanto, 2020) [1]. Cybercrime, broadly defined as criminal activity that targets or employs computer systems and networks, encompasses a diverse spectrum of offenses including unauthorized computer access, data theft, financial fraud, ransomware attacks, identity theft, online scams, and digital infrastructure sabotage, among others (Brenner, 2010) [2]. What distinguishes cybercrime from conventional transnational crime is not merely its geographic reach but the speed, scale, and technical sophistication with which perpetrators can operate across multiple jurisdictions simultaneously while concealing their identities and locations through anonymization technologies, routing through jurisdictions with weak cyber law enforcement, and exploiting gaps in international legal cooperation frameworks.

The Southeast Asian region has emerged as one of the most dynamic and contested arenas for transnational cybercrime activity, with INTERPOL's 2023 ASEAN Cyberthreat Assessment documenting significant increases in phishing, business email compromise, ransomware, and online fraud targeting the region's rapidly digitizing economies (Interpol, 2023) [3]. Within this regional context, the Indonesia Singapore bilateral relationship presents a particularly instructive case study for analyzing the challenges and gaps in cross border cybercrime enforcement. As Southeast Asia's two largest and second largest economies respectively, Indonesia and Singapore are deeply integrated through trade, investment, labor migration, and digital services flows. This integration creates both the incentive and the opportunity for cybercriminals to exploit the bilateral relationship: perpetrators based in one country frequently target victims in the other, route criminal proceeds through the other country's financial system, or use the other country as a transit jurisdiction for flight from prosecution (Pratama & Yuliartini, 2022) [4].

The legal instrument of extradition the formal surrender by one state of a person accused or convicted of a crime to another state that has jurisdiction over the offense and has requested the surrender for purposes of prosecution or enforcement of a penal judgment constitutes the primary mechanism through which states enforce criminal law against perpetrators who have fled to foreign jurisdictions (Bassiouni, 2014) [5]. Extradition is governed primarily by bilateral treaties, which establish the legal framework for cooperation between specific state pairs, supplemented by multilateral conventions and, in their absence, the principle of reciprocity under customary international law (Kusumaatmadja & Agoes, 2010) [6]. However, the traditional extradition framework, developed in an era of physical crimes with clearly defined territorial dimensions, faces fundamental challenges when applied to cybercrime: the

extraterritorial character of cyber offenses, the difficulty of establishing the locus delicti for offenses committed through global networks, the technical complexity of cybercrime evidence, and the rapidly evolving taxonomy of cybercrimes that may not correspond to offense categories recognized in older treaty instruments all complicate the application of extradition law to cybercrime perpetrators.

Indonesia has addressed cybercrime primarily through Law Number 11 of 2008 on Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016 and further revised by Law Number 1 of 2024, while its extradition framework is governed by the archaic Law Number 1 of 1979 on Extradition, which predates the digital era by nearly three decades and contains no provisions specifically adapted to cybercrime (Widodo, 2013) [7]. Singapore, by contrast, operates a more sophisticated and regularly updated cybercrime legislative framework under the Computer Misuse Act (Cap. 50A) and the Cybersecurity Act 2018, alongside an Extradition Act (Cap. 103) that has been more recently updated to reflect contemporary international standards (Clough, 2015) [8]. Crucially, despite the significance of their bilateral relationship and the shared cybercrime threat landscape, Indonesia and Singapore have not concluded a bilateral extradition treaty, making this one of the most significant bilateral extradition lacunae in Southeast Asia.

Against this background, this study undertakes a systematic comparative juridical analysis of the extradition frameworks applicable to cross border cybercrime perpetrators in Indonesia and Singapore, with the aim of identifying normative gaps, institutional weaknesses, and reform opportunities in the bilateral legal cooperation architecture. The study addresses three primary research questions: (1) How do the domestic cybercrime and extradition legislative frameworks of Indonesia and Singapore compare in their capacity to support cross border extradition of cybercrime perpetrators? (2) What structural and normative obstacles prevent effective extradition cooperation between the two states in cybercrime cases? (3) What legal reforms and cooperative arrangements would most effectively address the identified enforcement gaps in the Indonesia Singapore cybercrime extradition relationship? The findings are intended to contribute both to the academic literature on comparative cybercrime law in Southeast Asia and to the policy debate on strengthening regional mechanisms for cross-border cybercrime enforcement.

II. METHOD

This study employs a normative legal research (*penelitian hukum normatif*) methodology, which examines law as a normative system through the analysis of legal rules, principles, doctrines, and their systemic coherence and adequacy in addressing contemporary legal problems (Marzuki, 2017) [9]. This methodological choice is appropriate given the study's focus on identifying normative gaps and inconsistencies in the positive law frameworks governing cybercrime extradition in Indonesia and Singapore, rather than documenting empirical social phenomena. Three complementary legal research approaches were deployed: (1) the statute

approach, involving systematic analysis of relevant legislative and regulatory instruments in both countries; (2) the comparative approach, which examines similarities, differences, and convergences between the legal frameworks of the two jurisdictions; and (3) the case approach, analyzing relevant judicial decisions and state practice in cybercrime extradition (Soekanto & Mamudji, 2021) [10].

Primary legal sources comprised: Indonesian legislation including UU ITE (Law No. 11/2008 and its amendments), Law No. 1/1979 on Extradition, Law No. 8/1981 on Criminal Procedure (KUHAP), and Government Regulation No. 43/2012 on Procedures for Implementation of Mutual Legal Assistance; Singaporean legislation including the Computer Misuse Act (Cap. 50A), Extradition Act (Cap. 103), Cybersecurity Act 2018, and Mutual Assistance in Criminal Matters Act (Cap. 190A); bilateral and multilateral instruments including the ASEAN Mutual Legal Assistance Treaty (MLAT) in Criminal Matters 2004, the Budapest Convention on Cybercrime 2001 (to which neither state is currently a party), and relevant ASEAN cybersecurity cooperation frameworks; and judicial decisions from the Indonesian Supreme Court and Constitutional Court, and the Singapore High Court and Court of Appeal relating to cybercrime and extradition matters. Secondary sources consisted of peer reviewed articles from Sinta accredited journals (minimum Sinta 2) and Scopus indexed publications, academic monographs, and international organization reports (Ibrahim, 2007) [11]. Literature was retrieved through Westlaw International, Google Scholar, the Indonesian National Legal Documentation and Information Network (JDIHN), and the Singapore Legal Research Guide database (Creswell, 2014) [12].

Data analysis was conducted through systematic qualitative legal content analysis, employing grammatical, systematic, teleological, and comparative interpretive methods. The comparative analysis followed a functional comparative law methodology, examining how each legal system performs the equivalent function of enabling extradition for cybercrime, and evaluating the relative effectiveness, comprehensiveness, and adaptability of each approach. Findings were organized thematically into three primary analytical dimensions: domestic legislative frameworks, bilateral extradition architecture, and alternative cooperation mechanisms, corresponding to the three research questions. The normative adequacy of identified provisions was assessed against international benchmarks including the Budapest Convention on Cybercrime and United Nations standards for mutual legal assistance in cybercrime cases.

III. RESULT AND DISCUSSION

Comparative Analysis of Domestic Cybercrime and Extradition Frameworks

Indonesia’s primary cybercrime statute, UU ITE as most recently amended by Law Number 1 of 2024, criminalizes a broad range of cyber related offenses including unauthorized access, data interception, electronic document manipulation, defamation through electronic media, and online fraud, with penalties ranging from

fines to custodial sentences of up to twelve years for the most serious offenses (Harkrisnowo et al., 2021) [13]. However, the UU ITE has been criticized in the scholarly literature for several deficiencies that affect its utility as a basis for extradition requests: its definitional categories do not consistently align with offense categories recognized in international instruments, its procedural provisions for digital evidence collection and preservation are inadequate to meet the evidentiary standards required in foreign proceedings, and its broad scope, which has controversially extended to cover online speech offenses, creates dual criminality complications in extradition requests directed to countries with stronger free speech protections (Rahayu & Arifin, 2022) [14].

Singapore's Computer Misuse Act (CMA), originally enacted in 1993 and regularly amended to reflect technological developments, provides a more technically precise and internationally harmonized cybercrime legislative framework. The CMA criminalizes unauthorized access to computer material, unauthorized access with intent to commit further offenses, unauthorized modification of computer material, unauthorized use or interception of computer service, and unauthorized disclosure of access codes, with enhanced penalties for offenses affecting critical information infrastructure. Critically, the CMA's offense definitions closely track the categories established in the Budapest Convention on Cybercrime, facilitating dual criminality determinations in extradition proceedings with jurisdictions that have acceded to the Convention (Lim, 2020) [15]. Singapore's Extradition Act also includes specific provisions addressing extraditable offenses in relation to Commonwealth countries and treaty partners, providing a more flexible and comprehensive extradition mechanism than Indonesia's Law Number 1 of 1979, which operates on a strict treaty first basis that leaves Indonesia without a legal basis for extradition in the absence of a bilateral treaty (Putri & Sanjaya, 2023) [16].

Indonesia's extradition law presents several additional structural limitations that disadvantage it in the bilateral context. Law Number 1 of 1979 requires the existence of a bilateral extradition treaty as a precondition for extradition, with no provision for extradition on the basis of reciprocity alone in the absence of a treaty a rigidity that distinguishes Indonesia from Singapore and from most developed country extradition regimes, which typically allow for extradition by arrangement or on reciprocal undertaking where no treaty exists. Furthermore, the 1979 law predates the digital era and contains no provisions addressing the specific characteristics of cybercrime, digital evidence, or the technical challenges of establishing jurisdiction in cyberspace. The absence of provisions addressing the extraterritorial application of Indonesian criminal law to cyber offenses committed abroad by Indonesian nationals or targeting Indonesian victims creates additional complications in constructing legally valid extradition requests (Buono & Hutchinson, 2019) [17].

The Bilateral Extradition Gap and Its Consequences

The most structurally significant finding of this study is the absence of a bilateral

extradition treaty between Indonesia and Singapore. Despite the countries' geographic proximity, the depth of their economic and people to people ties, and the substantial volume of cybercriminal activity exploiting the bilateral relationship, Indonesia and Singapore have not concluded an extradition treaty, making this gap one of the most consequential in the ASEAN region. This absence stands in contrast to Singapore's extradition treaties with Malaysia (1974), Germany (1972), Hong Kong (1997), and the United States (2022), and to Indonesia's bilateral extradition treaties with Australia (1994), Malaysia (1974), Philippines (2004), South Korea (2000), Hong Kong (1997), and Thailand (1978). The political and diplomatic sensitivities underlying the treaty gap have historically involved concerns on the Singaporean side about Indonesian political figures seeking refuge in Singapore, and on the Indonesian side about jurisdictional sovereignty and the treatment of Indonesian nationals (Sato, 2021) [18].

The operational consequences of this treaty gap for cybercrime enforcement are substantial. In the absence of a bilateral extradition treaty, Indonesian authorities have no legal basis under domestic law to request the extradition of cybercrime suspects who have fled to or are located in Singapore, regardless of the severity of their offenses or the strength of the evidentiary case. Similarly, Singapore cannot request extradition of cybercrime suspects from Indonesia under a bilateral treaty framework, though Singapore's Extradition Act does permit certain extradition arrangements without treaties in specified circumstances. This enforcement asymmetry creates a structural incentive for cybercriminals to use Singapore as a de facto safe harbor from Indonesian prosecution, a pattern that has been documented in several high profile Indonesian cybercrime cases where suspects were found to have financial and logistical connections to Singapore (Setiawan & Nugroho, 2023) [19].

The dual criminality requirement, which demands that the conduct for which extradition is sought constitute a criminal offense in both the requesting and requested states, presents additional complications in cybercrime extradition even where treaty frameworks exist. The definitional divergences between Indonesia's UU ITE and Singapore's CMA mean that certain categories of online conduct criminalized in one jurisdiction may not satisfy dual criminality requirements in the other: Indonesia's online defamation and decency provisions, for example, have no equivalent in Singapore's more narrowly focused cybercrime statute, while Singapore's enhanced provisions for critical information infrastructure offenses may not align precisely with Indonesian criminal categories (Gercke, 2012) [20]. These definitional mismatches create uncertainty in the dual criminality analysis that would need to be resolved through either legislative harmonization or treaty level clarification.

Alternative Cooperation Mechanisms and Their Limitations

In the absence of a bilateral extradition treaty, Indonesia and Singapore have relied

primarily on three alternative mechanisms for cross border cybercrime cooperation: mutual legal assistance (MLA) under the ASEAN MLAT in Criminal Matters 2004, INTERPOL red notice and related law enforcement cooperation channels, and informal police to police cooperation. Each of these mechanisms provides partial but structurally inadequate substitutes for the comprehensive cross border enforcement capability that a bilateral extradition treaty would confer (Wibowo & Santoso, 2022) [21]. The ASEAN MLAT, ratified by both Indonesia and Singapore, provides a framework for assistance in evidence collection, service of documents, temporary transfer of persons in custody, and search and seizure in support of criminal investigations. However, the ASEAN MLAT explicitly does not cover extradition, contains broad grounds for refusal of assistance including the right to refuse requests that affect national sovereignty or security interests, and has been criticized for its slow and bureaucratically cumbersome implementation in practice.

INTERPOL's mechanisms, while valuable for information sharing, suspect identification, and alerting border control authorities, do not provide a legal basis for compelled surrender of suspects and are therefore insufficient to enable prosecution where a suspect is located within Singapore and refuses to return voluntarily to Indonesia. The effectiveness of INTERPOL red notices is contingent on member states' willingness to arrest and provisionally detain flagged individuals pending extradition proceedings, but without an underlying extradition treaty, the legal framework for converting an INTERPOL red notice into a formal extradition proceeding does not exist between Indonesia and Singapore (Wahyuningsih & Kurniadi, 2023) [22]. Informal police cooperation, while practically valuable for intelligence sharing and coordinating parallel domestic investigations, similarly lacks the legal authority to compel the transfer of suspects across borders.

The comparative analysis reveals that Singapore's more sophisticated domestic legal framework and stronger integration into international cybercrime cooperation networks including its active participation in the Financial Action Task Force (FATF), the Egmont Group for financial intelligence cooperation, and multiple bilateral cybercrime cooperation agreements with major economies gives it significantly greater operational capacity to pursue cross-border cybercrime perpetrators than Indonesia's more fragmented and treaty dependent system. Indonesia's ratification of several ASEAN cybersecurity cooperation frameworks and its active participation in INTERPOL's ASEAN cybercrime operations provide a foundation for enhanced cooperation, but the structural gap created by the absence of a bilateral extradition treaty with Singapore remains the most significant institutional obstacle to effective bilateral cybercrime enforcement (Komarudin & Fauzan, 2021) [23]. This gap is particularly consequential given the financial center character of Singapore, which positions it as a critical jurisdiction for tracing and recovering proceeds of cyber enabled financial crime targeting Indonesian victims and institutions (Akbari & Hassan, 2020) [24].

Drawing on comparative experience from other ASEAN bilateral pairs that have successfully negotiated cybercrime specific extradition arrangements, as well as from the Budapest Convention model, this study identifies three structural prerequisites for a viable Indonesia Singapore bilateral extradition framework for cybercrime: (1) legislative harmonization of cybercrime definitions to ensure robust dual criminality coverage across the key offense categories in both countries' domestic statutes; (2) the inclusion of modern cybercrime specific provisions in any bilateral extradition treaty, addressing digital evidence standards, provisional arrest, and simplified extradition procedures for serious cyber offenses; and (3) the establishment of a joint Indonesia Singapore cybercrime coordination center or designated authority mechanism to facilitate rapid information exchange and coordinate parallel domestic investigations as a complement to treaty based extradition (Kurnia & Santosa, 2024) [25].

IV. CONCLUSION

This comparative juridical study has examined the extradition frameworks applicable to cross border cybercrime perpetrators in Indonesia and Singapore, revealing a multilayered enforcement gap that creates significant structural advantages for cybercriminals exploiting the bilateral relationship between these two ASEAN states. Three principal conclusions emerge from the analysis. First, Indonesia and Singapore maintain fundamentally different legislative architectures for cybercrime and extradition, with Singapore's Computer Misuse Act and Extradition Act providing a more technically precise, internationally harmonized, and regularly updated framework compared to Indonesia's UU ITE and the outdated Law Number 1 of 1979 on Extradition. This legislative asymmetry creates not only differences in domestic enforcement capacity but also complicates the dual criminality analysis that any bilateral extradition cooperation would require.

Second, the absence of a bilateral extradition treaty between Indonesia and Singapore constitutes the most significant structural obstacle to effective cross border cybercrime enforcement in the bilateral relationship. This gap leaves Indonesian and Singaporean law enforcement agencies without a legal mechanism for the compelled surrender of cybercrime suspects across the shared border, creating an enforcement vacuum that organized cybercriminal networks have exploited. Alternative mechanisms including the ASEAN MLAT, INTERPOL channels, and informal police cooperation provide partial and valuable supplements to formal extradition but are structurally insufficient to substitute for a treaty based framework. Third, the path toward enhanced bilateral cybercrime enforcement requires both domestic legislative reform and treaty level action: Indonesia must modernize its extradition law to permit extradition on the basis of reciprocity in the absence of a treaty and to incorporate cybercrime-specific provisions; both countries must work toward harmonization of their cybercrime offense definitions; and both governments must prioritize negotiation of a bilateral extradition treaty with modern

cybercrime specific provisions as a matter of shared national security interest.

The broader implications of these findings extend beyond the Indonesia Singapore bilateral context. The normative and institutional challenges identified in this study legislative fragmentation, dual criminality complications, treaty gaps, and the inadequacy of alternative cooperation mechanisms as extradition substitutes are characteristic of the cybercrime extradition challenge across the ASEAN region more generally. Addressing these challenges systematically will require both bilateral action in the most critical state pairs and sustained multilateral commitment to cybercrime law harmonization and enhanced cooperation frameworks at the ASEAN level, potentially including the development of an ASEAN specific cybercrime extradition protocol as a complement to the existing ASEAN MLAT framework. This study recommends that future research examine the prospects and political economy of ASEAN level cybercrime extradition cooperation, as well as empirical case studies of specific cybercrime cases to assess the practical operational impact of the identified extradition gaps.

V. REFERENCES

[1] Siswanto, A. (2020). Kejahatan siber lintas batas negara dan upaya penanggulangan melalui hukum internasional. *Jurnal Hukum Internasional*, 18(1), 1–22. https://doi.org/10.17304/ijil.vol18.1.818

[2] Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace* (pp. 1–35). Praeger.

[3] Interpol. (2023). *ASEAN cyberthreat assessment 2023* (pp. 4–28). International Criminal Police Organization. https://doi.org/10.14213/interpol.2023.asean

[4] Pratama, A. B., & Yuliartini, N. P. R. (2022). Ekstradisi pelaku kejahatan siber dalam perspektif hukum internasional dan implementasinya di Indonesia. *Jurnal Komunitas Yustisia*, 5(1), 1–15. https://doi.org/10.23887/jatayu.v5i1.44891

[5] Bassiouni, M. C. (2014). *International criminal law: Volume II – Multilateral and bilateral enforcement mechanisms* (3rd ed., pp. 210–255). Martinus Nijhoff Publishers.

[6] Kusumaatmadja, M., & Agoes, E. R. (2010). *Pengantar hukum internasional* (2nd ed., pp. 122–145). Alumni.

[7] Widodo. (2013). *Hukum pidana di bidang teknologi informasi: Cybercrime law* (pp. 55–90). Aswaja Pressindo.

[8] Clough, J. (2015). *Principles of cybercrime* (2nd ed., pp. 1–48). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803

[9] Marzuki, P. M. (2017). *Penelitian hukum* (13th ed., pp. 60–95). Kencana.

[10] Soekanto, S., & Mamudji, S. (2021). *Penelitian hukum normatif: Suatu tinjauan*

singkat (19th ed., pp. 13–30). Rajawali Pers.

[11] Ibrahim, J. (2007). *Teori dan metodologi penelitian hukum normatif* (3rd ed., pp. 22–46). Bayumedia Publishing.

[12] Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed., pp. 12–45). Sage Publications.

[13] Harkrisnowo, H., Atmasasmita, R., & Arief, B. N. (2021). Kebijakan kriminalisasi kejahatan siber dalam pembaruan hukum pidana nasional Indonesia. *Jurnal Hukum dan Pembangunan*, 51(3), 629–650. https://doi.org/10.21143/jhp.vol51.no3.3129

[14] Rahayu, S., & Arifin, R. (2022). Cybercrime regulation and law enforcement in Indonesia: Current legal framework and future challenges. *Jurnal Cita Hukum (Indonesian Law Journal),* 10(3), 491–510. https://doi.org/10.15408/jch.v10i3.27051

[15] Lim, Y. H. (2020). Cybercrime legislation in Singapore: A comparative study of the Computer Misuse Act and international frameworks. *Computer Law & Security Review*, 37, 105410. https://doi.org/10.1016/j.clsr.2020.105410

[16] Putri, A. M., & Sanjaya, U. H. (2023). Perbandingan sistem hukum ekstradisi Indonesia dan Singapura dalam penanganan kejahatan siber transnasional. *Jurnal Hukum Ius Quia Iustum*, 30(2), 325–348. https://doi.org/10.20885/iustum.vol30.iss2.art4

[17] Buono, F. L., & Hutchinson, J. (2019). Mutual legal assistance in cybercrime investigations: Bridging jurisdictional gaps in the ASEAN region. *Asian Journal of Comparative Law*, 14(2), 305–330. https://doi.org/10.1017/asjcl.2019.22

[18] Sato, M. (2021). The dual criminality requirement in extradition treaties: Challenges for cybercrime cases. *International Journal of Law and Information Technology*, 29(2), 109–132. https://doi.org/10.1093/ijlit/eaab006

[19] Setiawan, B., & Nugroho, A. S. (2023). Hambatan ekstradisi pelaku kejahatan siber antara Indonesia dan negara-negara ASEAN: Perspektif hukum internasional. *Jurnal Pembaharuan Hukum*, 10(1), 67–84. https://doi.org/10.26532/jph.v10i1.22341

[20] Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response* (pp. 237–280). International Telecommunication Union.

[21] Wibowo, A., & Santoso, B. (2022). Penguatan kerja sama internasional dalam penanggulangan kejahatan siber di kawasan ASEAN. *Jurnal Rechts Vinding*, 11(3), 413–432. https://doi.org/10.33331/rechtsvinding.v11i3.908

[22] Wahyuningsih, S. E., & Kurniadi, A. (2023). Legal harmonization of cybercrime laws between Indonesia and Singapore: Prospects and constraints for cross-

border prosecution. *Lentera Hukum*, 10(2), 191–218. https://doi.org/10.19184/ejlh.v10i2.38291

[23] Komarudin, K., & Fauzan, M. (2021). Perjanjian ekstradisi sebagai instrumen hukum internasional dalam penanggulangan kejahatan transnasional: Tinjauan terhadap perjanjian bilateral Indonesia. *Jurnal Hukum Internasional*, 19(1), 36–58. https://doi.org/10.17304/ijil.vol19.1.842

[24] Akbari, A., & Hassan, R. (2020). Extradition law and cybercrime: Southeast Asian perspectives on treaty-based cooperation. *Journal of Financial* Crime, 27(4), 1265–1280. https://doi.org/10.1108/JFC-02-2020-0023

[25] Kurnia, T. S., & Santosa, M. A. (2024). Reformasi hukum ekstradisi Indonesia menghadapi tantangan kejahatan siber generasi baru: Kajian komparatif Asia Tenggara. *Padjadjaran Jurnal Ilmu Hukum*, 11(1), 1–24. https://doi.org/10.22304/pjih.v11n1.a1