LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. 11(2025)

THE MYTH OF LEGAL SOVEREIGNTY IN CYBERSPACE: WHY INDONESIA'S CYBERTERRORISM LAW IS A JURISDICTIONAL ILLUSION

[1]Nadiah Khaeriah Kadir, [2]Judhariksawan, [3]Syamsuddin Muhammad Noor, [4]Maskun

[1234] Faculty of Law, Hasanuddin University, Indonesia

nadiahkhaeriah@unhas.ac.id[1]

ABSTRACT

This article critically examines Indonesia's jurisdictional claims over cross-border cyberterrorism through the lens of international law, employing a conceptual analysis and a comparative approach with the United States and European Union. The research problem arises from Indonesia's reliance on domestic legislation to assert extraterritorial jurisdiction without adequate grounding in binding international norms or active participation in global norm-setting processes. The methodological framework combines a doctrinal normative legal method with conceptual reasoning to assess the theoretical basis of sovereignty in cyberspace, and comparative analysis to evaluate alternative jurisdictional models. Findings reveal that Indonesia's approach constitutes a jurisdictional illusion, a projection of digital sovereignty lacking both legitimacy and enforceability under international law. In contrast, the United States and European Union secure jurisdictional authority through alignment with international norms, multilateral cooperation, and adherence to the principle of non-intervention.

Keywords: *Cyberspace, Cyberterrorism, Jurisdiction, Sovereignty*

INTRODUCTION

The modern structure of public international law positions state sovereignty as the central principle underpinning the entire normative order in inter-state relations (Nurwahyuni et al, 2022). Within this framework, a state's legal authority applies solely within its territorial boundaries, unless explicit consent is granted by another state. Sovereignty not only serves as the foundation for the existence of domestic law but also as the parameter for determining the legality of a state's intervention in actions occurring beyond its jurisdiction. In theory, the principles of non-intervention and sovereign equality safeguard against the expansion of national laws in ways that could disrupt the international order (Syahrin, 2021). Jurisdiction cannot be claimed unilaterally to reach cross-border activities without a legal basis established through multilateral agreement.

Under traditional arrangements, international legal jurisdiction rests on spatial connection, nationality, or direct legal consequences for a state's interests. International legal instruments such as the United Nations Charter, the Vienna Convention, and various bilateral or multilateral treaties regulate the permissible scope of legal actions among states (Recio, 2022). Within this paradigm, jurisdictional reach is limited, exclusive, and fragmented. Law enforcement in relation to transnational events must be conducted through international cooperation mechanisms, rather than unilateral expansion of legal authority (Harkrisnowo, 2021). Public international law provides no legal space for a state to exercise jurisdiction beyond its sovereign boundaries except under the narrowly defined principle of universality, which itself depends on global consensus.

The global digital transformation has shaken the theoretical foundations of international law rooted in territoriality and sovereign exclusivity. Digital activities, including those threatening international security, may occur simultaneously across multiple regions without direct connection to a specific geographic location. Traditional jurisdictional principles in international law lose much of their practical force in this environment. Cyber intrusions targeting critical infrastructure, cross-border dissemination of extremist content, and digital network infiltrations by non-state armed groups represent activities not confined by conventional state boundaries. No comprehensive international legal framework currently governs jurisdiction over cross-border cyberattacks conducted by non-state actors.

As a global issue, cyberterrorism lacks an agreed definition under international law (Iftikhar, 2024). No international instrument explicitly defines or criminalizes cyberterrorism as a violation of

public international law. Existing conventions, such as the Budapest Convention, do not specifically regulate cyberterrorism, and the participation of developing states in drafting such instruments remains limited. As a result, there is no robust basis in public international law for attributing state responsibility to activities of cyberterrorism originating from, or involving actors located within, another state's jurisdiction. This legal vacuum reinforces the fragmentation of global cyber law, creating gaps exploited by non-state actors with high digital mobility.

When states respond to digital threats through domestic instruments with extraterritorial application, tensions between national sovereignty and international legal principles become more pronounced. Many states, including Indonesia, have begun formulating jurisdictional claims over transnational digital activities without first establishing international consensus (Coutinho, 2024). Such actions create potential legal conflicts between states, particularly when one state claims jurisdiction over activities conducted from the territory of another. These unilateral claims undermine the principle of non-intervention and open the way to normative conflict between domestic legal systems and international law. International law has yet to provide a solid framework for addressing jurisdictional claims in cyberspace, which by its very nature lacks a single sovereign owner.

Indonesia is among the states developing legal approaches to cross-border digital activities, including cyberterrorism, without a solid footing in international law. Its limited involvement in the formulation of international norms, low ratification of global cyber instruments, and unilateral approach to digital policy-making place Indonesia in a legally vulnerable position. In the absence of international agreement, states such as Indonesia tend to reproduce assertions of legal authority based on sovereignty claims unsupported by global legitimacy. Such practices are not only ineffective but also contradict the central principle of international law: that norms must be established through agreement among sovereign equals (Yusuvalieva, 2022).

When jurisdictional claims over cyberspace are constructed solely on domestic legal frameworks, a core question arises: does the state possess legitimate standing under international law to regulate and enforce laws over cross-border digital activities? The absence of substantive international agreements governing cyberterrorism renders such jurisdictional claims a form of unilateral legal expansion (Masyhar & Emovwodo, 2023). In public international law, extending jurisdiction without consensus constitutes a violation of the principles of non-intervention and respect for the sovereignty of other states. This condition produces the illusion that a state holds legal authority in cyberspace, when in fact such claims have no binding force beyond its territory without support from the global legal system.

Indonesia's jurisdictional claims over cyberterrorism originating abroad illustrate the imbalance between its national legal ambitions and the structural limitations of international law. Without active participation in global forums and engagement in norm-setting processes, the state cannot lawfully enforce claims over transnational cyberspace. This results in a gap in authority that cannot be filled unilaterally. When Indonesia attempts to regulate a domain beyond its legal control, it creates a projection of sovereignty lacking any foundation in international legal legitimacy. This is a form of jurisdictional illusion that not only weakens Indonesia's legal position at the global level but also exacerbates the fragmentation of international digital law.

Formulating legal arguments on cyberterrorism cannot proceed without testing the conceptual validity of jurisdictional claims advanced by states. Without a re-alignment of sovereignty paradigms in cyberspace, national regulations will continue to rest on flawed assumptions under international law. Developing states such as Indonesia risk reproducing ineffective legal frameworks that are misaligned with global norms based on consensus rather than unilateral claims. This research is therefore urgent in order to correct such approaches and provide an analytical framework more compatible with the structure of contemporary international law.

Existing studies on cyberterrorism have largely focused on technical measures or national policy responses (Shandler et al, 2022), while systematic examination from the perspective of international law remains limited (Sumadinata, 2023). A small number of works address digital security issues internationally, yet few engage critically and conceptually with jurisdictional claims.

The absence of an international definition of cyberterrorism generates normative ambiguity and restricts robust legal discourse at the global level. This study seeks to address that gap by offering a re-interpretation of the relationship between sovereignty, jurisdiction, and international law in the context of cyberterrorism.

The objective of this study is to critically examine Indonesia's jurisdictional claims over cyberterrorism from the perspective of international law, employing a conceptual approach and comparative analysis with the legal practices of the European Union and the United States. Its contribution lies in dismantling the myth of legal sovereignty in the digital domain and developing a conceptual framework for cyber jurisdiction grounded in equality, legality, and interstate cooperation within public international law. The article aims to strengthen the analytical foundation for the formulation of future transnational digital legal norms.

RESEARCH METHOD

This study adopts a doctrinal normative legal method with a conceptual and comparative approach. The conceptual approach is employed to critically examine the theoretical assumptions underlying state sovereignty in cyberspace. Meanwhile, the comparative approach is used to contrast Indonesia's legal posture with that of the United States and the European Union. Together, these methods enable a comprehensive critique of the illusion of jurisdictional authority in Indonesia's cyberterrorism law.

RESULT AND DISCUSSION

The Conceptual Fallacy of Sovereignty in Cyberspace

In classical international law, state sovereignty is constructed as the exclusive right to exercise jurisdiction over events occurring within a state's territorial boundaries. This principle emerged from the Westphalian tradition, which affirmed the supremacy of the state over its internal affairs and prohibited external interference in domestic matters (Bauder & Mueller, 2021). Within this structure, physical territory serves as the determinant of a state's lawful authority. Jurisdiction is grounded in the direct correlation between geographical space and legal power. No state may enforce its laws over foreign entities without violating the principle of non-intervention. This assumption remains deeply embedded in the framework of contemporary international law, despite the fact that modern patterns of global interdependence have blurred the functional boundaries of sovereignty itself.

Although cyberterrorism has become a prominent subject in global security discourse, no consensus has yet emerged in international law explicitly classifying it as a violation of public international law. There is no multilateral convention that definitively establishes the conceptual boundaries, criteria, or legal consequences of digital terrorism. While some efforts have been undertaken through United Nations General Assembly resolutions and other soft law instruments, these have not resulted in binding norms. Even in the *Tallinn Manual*, widely referenced in cyber law (Heinegg, 2022), cyberterrorism is not accorded a distinct status as an international crime triggering universal jurisdiction. The absence of normative recognition leaves states with limited capacity to invoke cyberterrorism as a lawful basis for cross-border jurisdiction under public international law. Without a robust normative foundation, jurisdictional claims over acts of cyberterrorism remain interpretative rather than imperative.

Cyberspace lacks spatial characteristics analogous to territorial domains (Ryngaert, 2023). Digital infrastructure such as servers, data storage systems, and network connectivity operates across borders without a singular geographic anchor. A single digital act may originate in one jurisdiction, be controlled from a second, stored on servers located in a third, and impact critical systems in a fourth. This technological distribution creates an environment that cannot structurally be governed through classical territorial approaches. When states attempt to impose legal authority on such a domain, the result is not an

expansion of sovereignty but a distortion of jurisdictional principles under international law.

Efforts to import territorial sovereignty models into the regulation of cyberspace expose the gap between legal concepts and technological realities. States that assert jurisdiction over cross-border digital activities without the foundation of international treaties or cooperative legal mechanisms erode the jurisdictional limits established by international law. The absence of a fixed spatial structure in cyberspace precludes reliance on traditional doctrines such as territoriality or nationality (Chatinakrob, 2024). When a state treats digital space as an extension of its territory, its legal argument is not only conceptually flawed but also generates serious consequences for an international legal order grounded in equality and non-intervention among states.

Indonesia's legal framework does not provide a distinct definition of cyberterrorism, instead implicitly subsuming it within the general category of terrorism under Law No. 5 of 2018. No normative boundaries exist to distinguish between digital attacks on information systems and physical acts meeting the elements of terrorism (Koto et al, 2022). This approach has legal implications: it employs ambiguous norms to construct jurisdictional claims over conduct not universally recognized as unlawful. As a result, Indonesia's expansion of digital jurisdiction to cover conduct domestically classified as cyberterrorism cannot secure international legitimacy, given the absence of normative equivalence in public international law. This reinforces the conclusion that Indonesia's jurisdictional posture is grounded in national law rather than in international legality, lacking global normative support.

At this juncture, the fundamental conceptual failure lies in the assumption that states retain exclusive control over legal activity in digital space, despite the fact that international law provides no legitimacy for unilateral claims over a non-territorial domain. When digital activity is classified as a threat to national security, states tend to extend their jurisdiction without resorting to reciprocal recognition or international negotiation. Such legal reasoning has no place in contemporary international law, which requires norm creation through multilateral processes. Replacing mutual consent with unilateral regulatory action risks undermining the very architecture of the international legal system.

The legal challenge to sovereignty claims in cyberspace is compounded by the absence of international consensus on the definition, scope, and normative regulation of digital activities deemed transnational threats. No binding global convention on cyberterrorism exists, and no universally recognized normative framework grants states the right to enforce laws over digital conduct occurring beyond their territory. In such circumstances, any jurisdictional claim premised on the assumption of legal authority in cyberspace operates without normative legitimacy under international law. This gap cannot be filled by domestic law, as national legal systems have no normative capacity to regulate beyond state borders without infringing on international legal principles.

Some states attempt to circumvent these limitations through doctrinal approaches such as the *"effects doctrine,"* which asserts that if a digital activity produces substantial effects within a state's domestic jurisdiction, that state has a legal basis to assert jurisdiction (Sukarmi et al, 2021). However, this approach enjoys no universal recognition in international law and becomes a source of interstate tension when applied unilaterally. Indonesia, for example, has adopted a similar approach in certain domestic regulations. Yet, absent an underlying framework of international cooperation, such claims carry no binding force under public international law, and other states are under no legal obligation to respect jurisdictional assertions they have not explicitly recognized.

Unilateral jurisdictional claims over digital space also distort the principle of respect for the sovereignty of other states. When a state unilaterally classifies a cyber activity as a security threat and seeks to enforce its laws against actors or data located within another jurisdiction, it normatively violates the principle of non-intervention. Under international

law, any action that intrudes into the jurisdiction of another state without consent whether physically or digitally constitutes a breach of sovereignty (Shi & Xu, 2021). There is no room within international norms to justify jurisdictional claims absent reciprocal consent. Such efforts are not only unenforceable but also risk generating broader legal conflicts among the states involved.

Tensions between digital sovereignty claims and the principles of international law become increasingly complex when states employ domestic legal instruments to justify actions affecting foreign jurisdictions. Many states have enacted legislation with extraterritorial reach in an effort to address digital activities deemed threats to national security. However, international law does not recognize a state's authority to apply its domestic laws beyond its territory without a treaty-based foundation or under the highly limited principle of universality (Criddle, 2024). Legislative models that unilaterally claim jurisdiction over cross-border cyber activities lack international legitimacy and reinforce criticism of legalistic approaches driven by sovereignty expansion rather than interstate legal cooperation.

Structurally, assertions of legal sovereignty in the digital domain also overlook the non-hierarchical character of the international legal system. There is no central authority in international law capable of imposing a singular interpretation of digital jurisdiction. While each state is free to develop domestic norms, such norms do not automatically apply in the international sphere. When a state seeks to implant legal authority into the global domain without consensus, it operates within a legitimacy vacuum, projecting unilateral claims without enforceable capacity. The absence of an international adjudicative mechanism specifically addressing digital jurisdiction further increases the susceptibility of this domain to normative disputes that cannot be structurally resolved.

Within this context, a conceptual illusion arises that a state can control cyberspace in the same manner it controls its physical territory (Farrand & Carrapico, 2022). This illusion is reinforced by normative approaches that fail to distinguish between the regulation of domestic digital infrastructure and the governance of transnational activities. While a state retains full authority over devices and digital services under its jurisdiction, such authority cannot be extended to domains beyond its technical or legal control (Kelton et al, 2022). When legal constructions fail to differentiate between administrative control and international legal authority, the state risks using domestic legal instruments to project power into spaces that do not fall under its sovereignty.

The consequences of this conceptual error extend beyond enforcement failures to the fragmentation of global legal norms. Each state that develops digital regulations based on unilateral interpretations of sovereignty widens normative gaps between states and weakens the potential for forming international consensus. When each state defines cyber threats and legal jurisdiction independently, legal interoperability across jurisdictions becomes impossible. Over time, this approach produces a contradictory global legal architecture, in which there is no mutual recognition, no stable dispute resolution mechanism, and no clarity on cross-border digital jurisdiction norms.

In the author's view, attempts by states to preserve or replicate the classical sovereignty model in the digital domain lack grounding in contemporary international law. Without a multilateral framework establishing legitimate definitions, boundaries, and mechanisms for digital jurisdiction, sovereignty claims over cyberspace remain legal projections without binding force. Misplacing sovereignty as the basis for legal expansion into a non-territorial domain creates a jurisdictional fallacy that is incompatible with technological realities and unjustifiable within an international legal structure that demands collective recognition of legal norms (Krisch, 2022). A new conceptual approach is therefore required one that aligns more closely with the unique characteristics of cyberspace and the fundamental principles of international law.

Indonesia's Cyberterrorism Law as Jurisdictional Overreach

Indonesia has responded to potential transnational digital threats through various domestic legal instruments designed to address cyber activities perceived as disruptive to national order. These instruments are formulated within a legalistic framework that seeks to classify cyberterrorism as a crime against the state. Through the Law on Electronic Information and Transactions (ITE Law) and Law No. 5 of 2018 on the Eradication of Terrorism, the state has adopted an approach that situates cyberterrorism within the spectrum of threats to sovereignty, thereby asserting the reach of national jurisdiction over offenders located abroad. This creates a regulatory framework granting the state wide authority to enforce laws against cross-border cyber conduct.

However, these regulations lack a solid foundation in international law. Jurisdictional claims over cyberspace particularly those targeting actors or entities located outside Indonesia are not supported by extradition treaties, mutual legal assistance agreements, or active participation in international conventions governing cyber security. The state has adopted a legal posture that assumes impacts on national interests are sufficient to trigger jurisdiction, without taking into account the principles of non-intervention or reciprocal recognition in the international system (Husch, 2023). This model is not only normatively weak but also operationally unworkable within the global legal structure, which depends heavily on multilateral consensus.

Indonesia's absence from key international cyber law-making forums weakens the state's legitimacy in asserting digital jurisdiction. The lack of ratification of the Budapest Convention, for example, reflects a tendency to construct a domestic legal system isolated from prevailing international norms (Bucaj & Idrizaj, 2024). While states party to the Convention build frameworks for technical and legal cooperation that enable information sharing and limited jurisdictional recognition, Indonesia has opted for a law enforcement model reliant solely on internal capacity. In a digitally interconnected world, such an approach is not only inefficient but also incompatible with the principle of legal coexistence under international law.

Indonesia's regulatory framework rests on the assumption that the state has the prerogative to prosecute cyber activities affecting domestic systems regardless of the perpetrator's geographic location or the infrastructure employed. This assumption is embedded in statutory provisions granting broad extraterritorial jurisdiction over foreign-based actors whose activities are deemed to threaten national security. Yet, international law does not recognize such jurisdictional claims absent treaty-based authority or a legitimate universality principle (Ntahiraja, 2022). The effects doctrine, sometimes invoked as justification, has no firmly established status in public international law and, when applied unilaterally, heightens the risk of legal conflict between states.

Beyond its divergence from fundamental principles of international law, Indonesia's cyberterrorism regulation reflects a flawed understanding of the technological structure of cyberspace. Enforcement against digital activities conducted through global infrastructure requires cross-border cooperation that cannot be achieved through domestic legal claims alone. In practice, identifying perpetrators, seizing data, and prosecuting offences are only possible through formal legal cooperation protocols. When a state attempts to enforce laws against entities beyond its jurisdiction without such infrastructure, its claims are not only unenforceable but also deprived of legal legitimacy.

Indonesia's legislative model also reveals a mismatch between normative ambition and operational capacity. On one hand, the regulations construct broad, extraterritorial jurisdictional claims; on the other, the state lacks the diplomatic, technical, and legal systems to support transnational law enforcement. This imbalance creates the legal illusion that the state can unilaterally control cyberspace. In reality, most foreign-origin cyber activities remain beyond the reach of Indonesia's legal authority. This illustrates a form of jurisdictional overreach driven less by the force of international law than by political desire to project domestic authority into spaces legally beyond reach (Pendle et al, 2024).

The consequences of such an approach extend beyond legal ineffectiveness to potential diplomatic tensions with other states. When Indonesia issues legal orders or extradition requests to prosecute actors in foreign jurisdictions without a bilateral or multilateral treaty basis, it risks violating the principle of non-intervention guaranteed by international law. Such actions may be construed as infringements on the sovereignty of other states, creating negative precedents in inter-state legal relations. In many cases, the targeted state may refuse cooperation or challenge the legitimacy of Indonesia's claims, thereby weakening the country's diplomatic standing and undermining its reputation in the global legal arena.

When a national legal system seeks to regulate domains factually beyond its authority, a contradiction emerges between legal ambition and the limits of legality itself. In international law, jurisdiction is determined not solely by state intent but by collective recognition within a binding normative framework (Chimni, 2021). Indonesia's regulations aimed at controlling cross-border cyberterrorism lack such recognition. The state cannot legitimately claim capacity to prosecute actors or access data located in foreign jurisdictions without first establishing treaties or cooperative mechanisms (Durham, 2021). Where legal processes are pursued in domains outside the state's legal structure, jurisdictional claims lose validity and become symbolic instruments devoid of binding force.

Moreover, Indonesia's unilateral approach generates long-term repercussions for international cyber governance (Manullang, 2022). When other developing states adopt similar strategies; expanding legal jurisdiction without international coordination, the result is not a coherent global system but overlapping, contradictory regulations. This fragmentation hinders the formation of shared norms, erodes the legitimacy of global digital law, and strengthens non-state actors who exploit the lack of order. In the framework of international law, norm creation cannot proceed through unilateral acts but must be developed through inter-state deliberation that ensures equality, consensus, and reciprocity. Indonesia has failed to secure a strategic position in such processes by relying more heavily on domestic legislation than on international legal diplomacy.

This conceptual flaw is compounded by the absence of any agenda to harmonize national legislation with evolving global norms. Indonesia has not positioned itself as an active contributor in the drafting of international instruments on cyber security, despite the fact that active participation is a fundamental prerequisite for attaining legitimacy in multilateral forums. As a result, the regulations it develops are exclusive in scope and disconnected from the dynamic architecture of international norms. In a pluralistic and decentralized international legal system, a state that remains absent from global norm-setting processes will struggle to justify its domestic regulations as part of the international legal order (Tourinho, 2021). This renders Indonesia's position in the global digital law arena passive, reactive, and strategically weak both normatively and politically.

Jurisdictional claims over cyberterrorism in Indonesia's regulatory framework are also not grounded in adequate analysis of the legal limits of universal jurisdiction under international law. Not all transnational crimes qualify as offences capable of triggering the application of the universal jurisdiction principle. Only a limited set of categories such as war crimes, genocide, and crimes against humanity can serve as a legitimate basis for such

claims. Cyberterrorism, at present, does not possess such legal status in international law. Consequently, any attempt to frame cyberterrorism as a justification for expanding jurisdiction without an international treaty basis faces serious challenges to its legitimacy under public international law. In this respect, Indonesia's legal arguments are disconnected from the global normative framework underpinning principles of cross-border jurisdiction.

Comparative Insights: United States and European Union Approaches

The United States and the European Union occupy dominant positions in the formulation of global legal norms, including in the regulation of cyberspace (Shahin, 2024). While adopting different approaches, both jurisdictions have developed frameworks designed to provide a solid legal basis for addressing transnational digital activities. Unlike Indonesia, which prioritizes the unilateral expansion of domestic legal authority without sufficient international recognition, the US and EU ground their legal instruments in international law and reinforce them through established networks of multilateral cooperation. This divergence creates a stark legal contrast and illustrates the extent to which international legitimacy can be secured through legal systems integrated with global norms.

The United States employs a broad jurisdictional model known as *long-arm jurisdiction*, enabling federal courts to assert authority over foreign entities where there is a substantial nexus to US national interests. This is supported by the *effects doctrine*, which holds that if an act produces significant effects within US territory or impacts US citizens, jurisdiction may be exercised even if the perpetrator is located abroad. However, this approach is not implemented in isolation. The US supplements its jurisdictional claims with diplomatic and international legal instruments, including bilateral extradition treaties, Mutual Legal Assistance Treaties (MLATs), and participation in global agreements such as the Budapest Convention on Cybercrime (Marcen, 2022).

In practice, the US applies digital jurisdiction selectively and within a framework of interstate negotiation. Law enforcement is not pursued solely through domestic legal authority but through international legal protocols that account for the sovereignty of other states. This demonstrates that while the US retains unilateral capabilities under the principles of effects and national interest, implementation remains within the boundaries of international legality, ensuring legitimacy for cross-border legal actions. As such, the US approach to jurisdictional expansion in cyberspace reflects not merely an extension of power, but active participation in shaping and maintaining the international legal architecture for cyber security.

By contrast, the European Union has developed a more cooperative approach grounded in the harmonization of laws among its member states. The EU's legal system rests on principles of mutual recognition and judicial cooperation, enabling the application of digital jurisdiction through structured and transparent mechanisms (Inchausti, 2024). Instruments such as the General Data Protection Regulation (GDPR) not only provide robust protection for EU citizens' personal data but also apply an extraterritorial reach to entities outside the EU that process such data (Kuner, 2023). This reach is grounded in legal connection through digital interaction, rather than unilateral expansion that disregards the sovereignty of other states.

In addition to the GDPR, the EU actively develops legal instruments that facilitate transnational cooperation in combating cybercrime. Its membership in the Budapest Convention evidences the EU's legal commitment to global standards governing cyber jurisdiction (Osula et al, 2022). Within this framework, the exercise of digital jurisdiction is transparent, legally documented, and traceable. This model is anchored in cooperation rather than dominance, and the EU's legal position affirms that cross-border jurisdiction must always adhere to the principles of legality and mutual recognition among states principles aligned with public international law.

The most striking difference between the EU and Indonesia lies in the use of

collectively developed legal infrastructure. While Indonesia relies on its national legal system to address transnational issues, the EU builds a regional legal system with operational capacity and international legitimacy. In the EU model, cyber jurisdiction is exercised not through coercive means but through norms widely accepted by the international community. This enables EU digital regulations to operate across borders without generating political resistance or violating the principle of non-intervention (Smith, 2023). The process underscores that the legitimacy of jurisdiction is determined not by the formal authority of national law, but by the extent to which the norm is accepted within the international legal system.

From the standpoint of international law, the US and EU share key similarities: both operate within the limits of international legality, rely on multilateral legal instruments, and prioritize formal cooperation mechanisms. While the US tends to be more assertive and unilateral in the construction of its legal framework, its enforcement practice still accounts for the structure of legal diplomacy (Hopewell, 2022). The EU, in contrast, emphasizes regional consolidation as the basis for collective legal authority. Although technically different, both approaches ensure the enforceability and global acceptance of digital norms. Indonesia's absence from such legal architectures explains its marginal position in the landscape of international digital law.

A fundamental element in both the US and EU approaches is their consistency in balancing jurisdictional claims with respect for international law. In the US legal system, even when extraterritorial jurisdiction is broadly applied, the state remains bound by international commitments limiting unilateral intervention in the legal domain of other states (Aryudhanty et al, 2023). Similarly, in the EU, all cross-border digital jurisdiction actions must proceed through legal procedures collectively recognized within the framework of regional cooperation (Pato & Pineau, 2021). This commitment demonstrates that digital legal authority is defined not solely by domestic capacity, but by active engagement in global decision-making structures.

Indonesia lacks the international legal foundation to adopt models comparable to those implemented by the US and EU. The absence of binding multilateral mechanisms, limited participation in normative forums, and a scarcity of bilateral and regional legal instruments render Indonesia's approach insular and unilateral (Auethavornpipat & Palmer, 2022). In public international law, such an approach reinforces normative isolation and reduces the effectiveness of national regulations in addressing transnational digital crimes. While the US and EU utilize domestic legal authority as a component of the global legal architecture, Indonesia treats it as a substitute for engagement in international norms a strategically counterproductive course.

The divergence in approaches also affects international perception and reception of jurisdictional claims. When the US or EU issues legal orders concerning cross-border cybercrime, other states are more inclined to respond constructively due to pre-established cooperation mechanisms. By contrast, when Indonesia submits similar requests, the target state can lawfully refuse on the grounds of lacking a valid legal basis. This underscores that the legitimacy of jurisdictional claims depends not on formal assertions of national law, but on their connectivity to established structures of international law. Indonesia's absence from this architecture undermines its digital legal claims, particularly in responding to cyberterrorism, in the eyes of the global community. International cooperation, therefore, remains a vital imperative for Indonesia (Maskun et al, 2021).

CONCLUSION

Indonesia's extraterritorial jurisdictional claims over cyberterrorism lack grounding in binding international norms, creating a structural disconnect between domestic political objectives and the normative limits international law. Through an analysis with the United States and European

Union, this study identifies such claims as a *jurisdictional illusion*, a projection of sovereignty in the digital sphere that lacks both legitimacy and practical enforceability. The comparison demonstrates that lawful and effective cyber jurisdiction requires formal alignment with international norms, participation in multilateral frameworks, and adherence to the principle of non-intervention.

The Indonesian approach, by expanding national law extraterritorially without reciprocal recognition, risks legal isolation, diplomatic friction, and diminished credibility in global cyber governance. As a contribution, this research advances the proposition that Indonesia must transition from unilateral legal expansion to active engagement in developing digital jurisdiction norms based on equality, legality, and international consensus, thereby securing both normative legitimacy and operational effectiveness.

REFERENCES

1. Aryudhanty, Desvia Dwi, et al. (2023). Pros and Cons of Application of Extraterritorial Jurisdiction in International Law: Various Practices in Southeast Asian Countries. *International Law Discourse in Southeast Asia, 2(1), 57-74.* https://doi.org/10.15294/ildisea.v2i1.58389.
2. Auethavornpipat, Ruji & Palmer, Wayne. (2022). Indonesia's Promotion of UN Migrant Protection Norms in ASEAN. *Pacific Affairs, 95(1), 75-97.* https://doi.org/10.5509/202295175.
3. Bauder, Harald & Mueller, Rebecca. (2021). Westphalian Vs. Indigenous Sovereignity: Challenging Colonial Territorial Governance. *Geopolitics, 28(1), 1-18.* https://doi.org/10.1080/14650045.2021.1920577.
4. Bucaj, Enver & Idrizaj, Kenan. (2024). The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. *Multidisciplinary Reviews, 8(1), 1-10.* https://doi.org/10.31893/multirev.2025024.
5. Chatinakrob, Thanapat. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law, 23(1), 25-72.* https://doi.org/10.1093/chinesejil/jmae005.
6. Chimni, B.S. (2021). The International Law of Jurisdiction: A TWAIL Perspective. *Leiden Journal of International Law, 35(1), 29-54.* https://doi.org/10.1017/S0922156521000534.
7. Coutinho, Ricardo. (2024). Legal Space of Modern Political Life: Digital Law and International Governance. *Science of Law, 2, 1-8.* https://doi.org/10.55284/sol.v2024i2.127.
8. Criddle, Evan J. (2024). Extraterritoriality's Empire: How Self-Determination Limits Extraterritorial Lawmaking. *The American Journal of International Law, 118(4), 607-658.* https://doi.org/10.1017/ajil.2024.33.
9. Durham, Helen. (2021). Counterterrorism, Sanctions and War. *International Review of the Red Cross, 103, 1-9.* https://doi.org/10.1017/S1816383121000898.
10. Farrand, Benjamin & Carrapico, Helena. (2022). Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity. *European Security, 31(3), 435-453.* https://doi.org/10.1080/09662839.2022.2102896.
11. Harkrisnowo, Harkristuti. (2021). Transnational Organized Crime: Dalam Perspektif Hukum Pidana dan Kriminologi. *Indonesian Journal of International Law, 1(2), 323-341.* https://doi.org/10.17304/ijil.vol1.2.408.
12. Heinegg, Wolf Heintschel von. (2022). Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics. *Journal on the Use of Force and International Law, 9(1), 229-240.* https://doi.org/10.1080/20531702.2021.1963578.
13. Hopewell, Kristen. (2022). Beyond U.S.-China Rivalry: Rule Breaking, Economic Coercion, and the Weaponization of Trade. *American Journal of International Law, 116, 58-63.* https://doi.org/10.1017/aju.2022.3.
14. Husch, Pia. (2023). Non-Intervention Thresholds in Cyberspace – In the Shadow of the Sovereignty Debate?. *Nordic Journal of International Law 92(3), 371-393.* https://doi.org/10.1163/15718107-92030001.
15. Iftikhar, Saman. (2024). Cyberterrorism as a Global Threat: A Review on Repercussions and

Countermeasures. *PeerJ Computer Science, 10, 1-32.* https://doi.org/10.7717/peerj-cs.1772.
16. Inchausti, Fernando Gascon. (2024). The New Regulation on the Digitalisation of Judicial Cooperation in the European Union: Something Old, Something New, Something Borrowed and Something Blue. *ERA Forum, 24, 535-552.* https://doi.org/10.1007/s12027-024-00782-z.
17. Kelton, Maryanne, et al. (2022). Virtual Sovereignty? Private Internet Capital, Digital Platforms and Infrastructural Power in the United States. *International Affairs, 98(6), 1977-1999.* https://doi.org/10.1093/ia/iiac226.
18. Koto, Ismail, et al. (2022). Provisions of Legal Protection for Terrorism Victim in Order to Realize Constitution Order. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi, 5(2), 243-252.* https://doi.org/10.24090/volksgeist.v5i2.6939.
19. Krisch, Nico. (2022). Jurisdiction Unbound: (Extra)territorial Regulation as Global Governance. *European Journal of International Law, 33(2), 481-514.* https://doi.org/10.1093/ejil/chac028.
20. Kuner, Christopher. (2023). Protecting EU Data Outside EU Borders Under the GDPR. *Common Market Law Review, 60(1), 77-106.* https://doi.org/10.54648/cola2023004.
21. Manullang, Sardjana Orba. (2022). The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws. *Society, 10(2), 390-403.* https://doi.org/10.33019/society.v10i2.482.
22. Marcen, Ana Gascon. (2022). The Push for the International Regulation of Cross-Border Access to Electronic Evidence and Human Rights. *Cuadernos de Derecho Transnacional, 15(1), 385-402.* https://doi.org/10.20318/cdt.2023.7545.
23. Maskun, et al. (2021). Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with it. *Jambe Law Journal, 4(2), 131-150.* https://doi.org/10.22437/jlj.4.2.131-150.
24. Masyhar, Ali & Emovwodo, Silaas Oghenemaro. (2023). Techno-Prevention in Counterterrorism: Between Countering Crime and Human Rights Protection. *Journal of Human Rights, Culture and Legal System, 3(3), 625-655.* https://doi.org/10.53955/jhcls.v3i3.176.
25. Ntahiraja, Bernard. (2022). The Legality and Scope of Universal Jurisdiction in Criminal Matters. *Nordic Journal of International Law, 91, 390-418.* https://doi.org/10.1163/15718107-91030005.
26. Nurwahyuni, Sumartini, Sitti & Kholik, Saeful. (2022). Kedudukan Hukum dalam Perspektif Negara Hukum Modern. *Jurnal Suara Hukum, 4(1), 224-242.* https://doi.org/10.26740/jsh.v4n1.p224-242.
27. Osula, Anna-Maria, et al. (2022). EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology, 16(1), 89-123.* https://doi.org/10.5817/MUJLT2022-1-4.
28. Pato, Alexia & Pineau, Elena Rodriguez. (2021). Cross-Border Data Protection Through Collective Litigation: A EU Legal Maze?. *European Data Protection Law Review, 7(4), 550-559.* https://doi.org/10.21552/edpl/2021/4/10.
29. Pendle, Naomi, et al. (2024). Remaking the Law to Protect Civilians: Overlapping Jurisdictions and Contested Spaces in UN Protection of Civilian Sites. *Journal of Intervention and Statebuilding, 18(1), 43-60.* https://doi.org/10.1080/17502977.2023.2226028.
30. Recio, Maria Eugenia. (2022). Shaping REDD+: Interactions Between Bilateral and Multilateral Rulemaking. *Journal of Environmental Law, 34, 83-106.* https://doi.org/10.1093/jel/eqab025.
31. Ryngaert, Cedric. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal, 24, 537-550.* https://doi.org/10.1017/glj.2023.24.
32. Shahin, Jamal. (2024). Dancing to the Same Tune? EU and US Approaches to Standards Setting in the Global Digital Sector. *Journal of European Integration, 46, 1111-1131.* https://doi.org/10.1080/07036337.2024.2398430.
33. Shandler, Ryan, et al. (2022). Cyber Terrorism and Public Support for Retaliation: A Multi-Country Survey Experiment. *British Journal of Political Science, 52, 850-868.* . https://doi.org/10.1017/S0007123420000812.
34. Shi, Jianzhong & Xu, Ming. (2021). Visualizing International Studies on Cyberspace Sovereignty: Concept, Rationality, and Legimacy. *International Journal of Legal Discourse,*

6(2), 251-289. https://doi.org/10.1515/ijld-2021-2056.

35. Smith, Hanna. (2023). The Geopolitics of Cyberspace and the European Union's Changing Identity. *Journal of European Integration, 45, 1219-1234.* https://doi.org/10.1080/07036337.2023.2277329.
36. Sukarmi et al. (2021). The Qualified Effects Doctrine in the Extraterritorial of Competition Law Application: An Indonesia Perspective. *Sriwijaya Law Review, 5(2), 192-204.* https://doi.org/10.28946/slrev.Vol5.Iss2.1050pp192-204.
37. Sumadinata, Widya Setiabudi. (2023). Cybercrime and Global Security Threats: A Challenge in International Law. *Russian Law Journal, 11(3), 438-444.* https://doi.org/10.52783/rlj.v11i3.1112.
38. Syahrin, M. Alvi. (2021). The Principle of Non-Refoulement As Jus Cogens: History, Application, and Exception in International Refugee Law. *Journal of Indonesian Legal Studies, 6(1), 53-82.* https://doi.org/10.15294/jils.v6i1.43350.
39. Tourinho, Marcos. (2021). The Co-Constitution of Order. *International Organization, 75(2), 258-281.* https://doi.org/10.1017/S0020818320000466.
40. Yusuvalieva, Rakhima. (2022). Formation of the Equality Principle as a General Principle of Law. *Yurisprudence, 2(2), 152-165.* https://doi.org/10.51788/tsul.jurisprudence.2.2./NEYW8712.