

Extraterritorial Jurisdiction in The New Indonesian Penal Code: Addressing Transnational Cybercrime

Aliv Izzul Haq¹, Joko Setiyono²

^{1,2}Master of Law, Faculty of Law, Diponegoro University, Semarang, Indonesia

ABSTRACT: The digital era has fundamentally transformed transnational organized crime, positioning cybercrime as a borderless threat that challenges conventional territorial jurisdiction. This study employs normative juridical research, utilizing statute and conceptual approaches, to examine the paradigm shift toward extraterritorial jurisdiction and its enforcement challenges under Indonesia's New National Criminal Code (Law Number 1 of 2023). The findings reveal that the unique characteristics of cybercrime such as extreme anonymity, exponential scalability, and cross jurisdictional fragmentation mandate this jurisdictional expansion, aligning with global frameworks like the 2001 Budapest Convention. The New Penal Code facilitates this through Articles 4 to 8, notably Article 4(e), which explicitly protects national digital interests globally. However, its application encounters significant challenges, primarily the operational limits of foreign state sovereignty and the Code's broad formulation that lacks technical specificity. Consequently, this penal reform remains transitional, relying heavily on *lex specialis* legislation such as the Electronic Information and Transactions (ITE) and Personal Data Protection (PDP) laws. Ultimately, effective enforcement requires robust regulatory synchronization and enhanced international cooperation mechanisms, such as Mutual Legal Assistance (MLA).

KEYWORDS: Extraterritorial Jurisdiction; Transnational Cybercrime; Indonesia Penal Code.

I. INTRODUCTION

Transnational organized crime is a well-established phenomenon; however, the digital age has fundamentally transformed its operational dynamics, compelling a comprehensive and synchronized international legal framework. Furthermore, the pervasive and deceptive nature of these offenses characterized by complex syndicate structures and the exploitation of jurisdictional ambiguities mandates unified global intervention (Khan, 2024).

The advent of the digital era has catalyzed fundamental transformations across various sectors of human life ranging from the flow of information and communication to commercial and educational activities through the optimization of technology and the internet. Despite the myriad conveniences offered, massive digitalization has also given rise to crucial challenges and negative implications, with one of the primary threats being the emergence of cybercrime.

Driven by the rapid escalation of information technology, cybercrime constitutes a criminal offense that exploits computer systems and networks as its primary instruments. Given that its operational medium is the inherently borderless internet, the scope of this crime is no longer exclusively subject to the jurisdiction of a single sovereign state. It is precisely this borderless characteristic that justifies the classification of cybercrime under the transnational crime regime (Situmeang, 2020).

Transnational crime constitutes an act or activity committed beyond the territorial boundaries of a single state. Cybercrime, being a subset of transnational crime, inherently correlates with extraterritorial jurisdiction. The concept of extraterritorial jurisdiction is addressed in the 2001 Convention on Cybercrime in Budapest. This convention comprehensively regulates various matters, ranging from cyber offenses to the settlement of disputes between states.

Cybercrime represents an increasingly alarming modern trend. This category encompasses a wide array of criminal activities committed via the internet or other digital means, including identity theft, financial fraud, hacking, and the distribution of illegal digital content. The transnational nature of the internet makes cybercrime exceptionally challenging to combat, as perpetrators and victims are frequently located in different jurisdictions (Khan, 2024).

The phenomenon of cybercrime is currently experiencing a significant surge in prevalence within society. Empirical findings from the Association of Indonesian Internet Service Providers (APJII) derived from a survey of 8,720 respondents across 38 provinces conducted between December 18, 2023, and January 19, 2024 corroborate the escalation of these data security threats. Comparative data indicate a sharp spike in various digital crime *modi operandi* from 2023 to 2024. Incidents of online fraud skyrocketed from 10.30% to 32.50%, concurrent with rising cases of personal data theft (from 7.96% to 20.97%) and device

malware infections (from 9.28% to 19.31%). Furthermore, application accessibility issues also increased from 5.55% to 10.04%, alongside various other cases (from 2.55% to 5.32%). Ironically, the escalation of these crimes is directly proportional to the public's lack of digital literacy; this is evidenced by the surging percentage of respondents who lack an understanding of data security concepts, which jumped from 42.45% in 2023 to 74.59% in 2024 (APJII, 2024)

The historical trajectory of International Criminal Law sparked by global security threats ranging from Napoleon's exile to the landmark Nuremberg Trials established the bedrock for contemporary accountability regarding war crimes, genocide, and crimes against humanity. Nevertheless, this foundational framework was inherently limited, as it primarily targeted the most egregious atrocities committed during armed hostilities and under despotic regimes (Tuliakov, 2025).

Cybercrime is a scourge that devastates the lives of countless individuals worldwide, possessing a significant transnational component. Even though national and international regulations have been in place for decades, the scale and scope of this phenomenon continue to expand, signaling that the current legal responses are fundamentally failing (Arnel & Faturoti, 2023).

The fight against transnational organized crime is underpinned by a series of key international laws and treaties, which provide the legal foundation for international cooperation and law enforcement. These instruments are vital in establishing standards and guiding the actions of states in their efforts to combat various forms of cross border criminal activities (Khan, 2024). In light of the aforementioned points, the handling and enforcement of cybercrime, as a cross border offense, inevitably intersect with the issue of state jurisdiction. The existence of state jurisdiction is inextricably linked to the principle of state sovereignty, which serves as a fundamental attribute of a sovereign entity. This jurisdictional authority emerges as a logical manifestation of sovereignty and the exclusive rights inherent in a state. Consequently, a state exercises absolute jurisdictional control within its territorial boundaries, given that such sovereignty represents the ultimate legitimacy and authority over all aspects of state affairs within its spatial scope (Kusumaatmadja & Agoes, 2003).

The enactment of Law Number 1 of 2023 concerning the Criminal Code (the National Criminal Code) inevitably brings about changes to its substantive provisions, including the concept of jurisdiction in criminal matters. The enactment of Law Number 1 of 2023 concerning the Criminal Code marks a crucial milestone in the evolution of penal reform in Indonesia. This codification effort serves as a manifestation of decolonization to shed the colonial legacy of the *Wetboek van Strafrecht* (WvS), the existence of which is deemed no longer compatible with contemporary socio-political dynamics. The reconstruction of these penal principles is fundamentally catalyzed by the transformation of humanitarian values to realize a law enforcement paradigm that is not only effective and oriented towards substantive justice, but also humanistic, embodying the spirit of progressive law that aligns with the nation's socio-cultural roots (Adriansyah & Edrisy, 2025).

Three philosophical and pragmatic foundations underpin the urgency of reforming the Criminal Code in Indonesia: the political, sociological, and practical dimensions. Politically, the codification of the National Criminal Code constitutes a manifestation of the sovereignty and identity of an independent nation, as well as a decolonization effort to shed the colonial symbols inherent in the legal products of the past. On a sociological level, the colonial legacy of the *Wetboek van Strafrecht* (WvS) is deemed to have lost its footing in contemporary societal realities; consequently, the new penal system must be rooted in the values living and developing within society (the living law). Meanwhile, from a practical perspective, this regulatory transition is essential to minimize disparities in law enforcement and prevent judicial misinterpretations that frequently arise due to the translation constraints of the original Dutch text (Amrani, 2019).

Furthermore, the urgency of this reform is also driven by several structural problems: the obsolescence of the *Wetboek van Strafrecht* (WvS) in the face of accelerating national criminal law, the fading centrality of the Criminal Code due to the proliferation of sectoral laws that triggers a dualism in the justice system, and regulatory overlap caused by the duplication of norms. Essentially, this penal reform is propelled by four fundamental pillars. First, decolonization, namely the substitution of colonial value systems with the philosophical roots of the nation's identity. Second, democratization, manifested in the alignment of the law with human rights principles. Third, consolidation, taking the form of an integrated re-codification that unifies general and specific penal provisions into a single instrument. Fourth, adaptation and harmonization, which ensures the flexibility and responsiveness of criminal law to the constellation of scientific advancements and global values (Amrani, 2019).

Based on the aforementioned elaboration, it is evident that the enactment of the National Criminal Code brings about significant transformations. Within the context of this paper, substantial changes inevitably occur regarding the concept of criminal jurisdiction. This is a response to global transformations that yield not only positive advancements but also adverse consequences, such as the emergence of crimes that no longer operate exclusively within a single national territory. Instead, these offenses penetrate the jurisdictions of other states, inherently involving international actors. Transnational cybercrime, in particular, demands specialized handling, given that such offenses transcend state jurisdiction as a direct consequence of global development. Therefore, this paper, entitled "Extraterritorial Jurisdiction in the New Indonesian Penal Code: Addressing Transnational Cybercrime," comprehensively examines two primary issues: first, how The Characteristics of Transnational Cybercrime Necessitate a Paradigm Shift from Territorial to Extraterritorial Jurisdiction, and second, The Application and Challenges of Enforcing Extraterritorial Jurisdiction under the New Indonesian Penal Code in Addressing Transnational Cybercrime.

II. METHODS

Methodologically, this study relies on a comprehensive literature review (library research) without involving field observation, representing the definitive characteristic of normative juridical legal research. The central focus of this research is a critical examination of the architecture of legal norms enshrined in Law Number 1 of 2023. To generate a holistic abstraction concerning the implications and paradigm shifts of contemporary criminal law, this study integrates two analytical tools. The first instrument is the statute approach, tasked with dissecting the legitimacy and the positive text structure of the National Criminal Code. The second instrument, the conceptual approach, is utilized to delve into the theoretical foundations of crucial norms, primarily regarding the expansion of extraterritorial jurisdiction accommodated by the new penal regime (Solikin, 2021).

The data sources in this normative research rely entirely on secondary data, which are restricted into a three tiered hierarchy of legal materials. At the first stratum, primary legal materials are extracted directly from the principal legislative instrument, namely Law Number 1 of 2023 concerning the Criminal Code. Subsequently, secondary legal materials are compiled from academic discourse found in literature, encompassing both books and journals. As a complement, tertiary legal materials such as encyclopedias and legal lexicons serve as supporting explanatory instruments. This data acquisition procedure is operationalized through library research, wherein the process of searching, tracking, and reviewing literature is executed comprehensively. This methodological step aims to map the dynamics of contemporary criminal law, with a primary focus on the construction of extraterritorial jurisdiction following the enactment of the New Criminal Code. The entire legal corpus is then dissected using qualitative analysis with a descriptive analytical approach to produce a holistic interpretation of the norms.

III. RESULT AND DISCUSSION

1. The Characteristics of Transnational Cybercrime Necessitate a Paradigm Shift from Territorial to Extraterritorial Jurisdiction

From a legal perspective, cybercrime herein is constructed as unauthorized and unlawful intrusion or illegal access to computing systems and internet networks. The penal emphasis of this offense hinges entirely on the unlawful entry itself, irrespective of whether the infiltration results in damage, manipulation, or data alteration within the targeted facility (Edrissy, 2019).

The global legal foundation for extraterritorial jurisdiction has been comprehensively accommodated through the Convention on Cybercrime (the 2001 Budapest Convention). This convention constructs a holistic legal instrument, ranging from the conceptualization of criminal offenses to cross-border dispute settlement mechanisms. Systematically, the anatomy of the convention can be mapped into several primary clusters. First, the terminological provisions (Article 1), which define computing systems, communication traffic data, and service providers. Second, the substantive criminal law cluster (Articles 2–13), which criminalizes various cyber offenses such as illegal access and interception, data and system interference, misuse of devices, fraud, child pornography, and copyright infringement along with their corresponding sanctions and corporate liability. Third, the procedural law cluster (Articles 14–21), which governs evidentiary procedures, ranging from data preservation, production orders, and search and seizure, to real time data interception. Fourth, as a crucial epicenter, Article 22 specifically formulates the authority and jurisdictional limits in the enforcement of cybercrime. Fifth, the international cooperation regime (Articles 23–35), which establishes the principles of extradition, Mutual Legal Assistance (MLA), and joint investigative authorities. Finally, the convention concludes with administrative provisions (Articles 36–48), encompassing ratification, amendments, and dispute resolution among the parties (Europe, 2001).

A multitude of states, both within and beyond Europe, have ratified the Convention on Cybercrime (the Budapest Convention), bringing the current number of state parties to over 80. Conversely, two states, Ireland and South Africa, remain signatories that have yet to ratify the instrument. Moreover, in relation to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, the protocol garnered 46 signatures as of June 20, 2024. Although widely signed, only a handful of nations have successfully completed the official ratification process for this protocol thus far.

As a manifestation of legal sovereignty in responding to the escalation of cybercrime, Indonesia has comprehensively reconstructed its regulatory architecture. This normative framework is underpinned by the existence of *lex specialis* regulations, namely the Law on Electronic Information and Transactions (Law Number 11 of 2008, recently updated by Law Number 1 of 2024), alongside the full implementation of Law Number 27 of 2022 on Personal Data Protection (PDP). Furthermore, to accommodate the prosecution of crimes transcending territorial boundaries, law enforcement instruments are fortified by Law Number 1 of 2006 concerning Mutual Legal Assistance in Criminal Matters. Serving as the culminating pillar, cybercrime offenses have now been entirely consolidated into the general penal regime through the enactment of the National Criminal Code, embodied in Law Number 1 of 2023 (Gunawan, 2024).

With reference to the substantive criminal law provisions in the Convention on Cybercrime (the Budapest Convention), the spectrum of cyber offenses codified in Articles 2 through 11 can be distilled into ten typologies of offenses. Doctrinally, these ten violations can be classified into several primary clusters: first, offenses against the confidentiality and integrity of systems (comprising illegal access, illegal interception, data and system interference, and the misuse of devices); second, economically

Extraterritorial Jurisdiction in The New Indonesian Penal Code: Addressing Transnational Cybercrime

motivated crimes (computer related forgery and fraud); third, content-related offenses (child pornography); fourth, intellectual property violations (copyright infringement); and fifth, inchoate and participatory offenses, namely liability for the attempt or aiding and abetting in the commission of cybercrimes (Europe, 2024).

The transformation of information technology in the digital era has dismantled conventional territorial barriers, positioning cybercrime strictly as an inherently borderless transnational threat. The fact that perpetrators can execute their crimes across multiple jurisdictions without the need for physical relocation carries severe implications for the legal sovereignty of a state. This reality imperatively compels states to set aside jurisdictional egos and forge robust global cooperation. Furthermore, overarching instruments such as the Convention on Cybercrime have explicitly laid the legitimate groundwork for the application of extraterritorial jurisdiction to address the complexities of such cross-border offenses (Nabila, et.al, 2024). Consequently, there is a clear paradigm shift in addressing transnational cybercrime, moving away from a traditional territorial basis toward extraterritorial jurisdiction. This evolution is driven by its nature as a profoundly borderless threat one that offenders can execute across various jurisdictions without any physical movement, inflicting severe consequences on state sovereignty.

As a modern criminal entity, cybercrime exhibits a stark differentiation in its characteristics compared to conventional offenses. Its inherent traits such as the anonymity of legal subjects, the massive escalation in crime distribution, and its capability to breach transnational jurisdictional boundaries render it incompatible with being addressed solely through orthodox criminal law instruments. Responding to these challenges in the digital realm, Indonesia's positive legal system, as previously mentioned, has accommodated several specific regulatory instruments anchored in Law Number 11 of 2008 in conjunction with (*juncto*) Law Number 1 of 2024 concerning Electronic Information and Transactions (the ITE Law). This regulatory constellation is operationally fortified through Government Regulation Number 71 of 2019, which governs the Operation of Electronic Systems and Transactions (Anastasya, et.al., 2024)

The complexity of cybercrime is inextricably linked to the high degree of perpetrator anonymity, characterizing it as a 'faceless crime'. Criminologically, this offense requires neither physical encounters nor identity disclosures between the perpetrator and the victim. Suspects can freely camouflage their digital footprints by exploiting proxy networks, encryption technologies, and penetrating the dark web. This intricate situation directly disrupts the effectiveness of investigation and law enforcement processes, regardless of the magnitude of the material losses incurred. Furthermore, the *modus operandi* of these criminal acts is frequently orchestrated in an automated manner utilizing bots, scripts, or autonomous software meaning that the execution of the crime no longer demands persistent human intervention (Rakha, 2024).

The cross jurisdictional nature of cybercrime introduces a profound disruption to conventional criminal law frameworks, which are rigidly anchored in the principle of territoriality. In practice, this offense frequently fractures the *locus delicti*; the perpetrator, the victim's domicile, and the exploited server infrastructure may be distributed across entirely different sovereign states. Such operational fragmentation inevitably culminates in jurisdictional clashes between sovereignties. As a logical consequence, the acceleration of law enforcement frequently encounters impasses driven by disparities in national legal systems, friction over data privacy policies, and the rigid boundaries of law enforcement authorities in respective countries (Cahyono, et.al., 2025).

Another defining characteristic of cybercrime lies in the acceleration and escalation capacity of its attacks. Diametrically opposed to conventional offenses, which are constrained by spatial and temporal boundaries, digital offenses possess the capability to propagate simultaneously across millions of computing infrastructures in a mere fraction of a second. The most extreme manifestation of this pattern is exemplified by Distributed Denial of Service (DDoS) attacks that paralyze public service systems, as well as the widespread distribution of malware that inflicts massive destruction on crucial databases. The logical implication of this exponential escalation and acceleration culminates in a vastly extensive and destructive spectrum of damage, which frequently transcends standard mitigation controls (Cahyono, et. al, 2025).

Based on the preceding elaboration, it is patently clear that cybercrime falls within the category of cross-border (transnational) offenses, thereby necessitating the application of extraterritorial jurisdiction in its handling and enforcement. This requirement is driven by several key aspects, namely the anonymity of legal subjects, the massive escalation of the crimes, and the capability to breach transnational jurisdictional boundaries.

2. The Application and Challenges of Enforcing Extraterritorial Jurisdiction under the New Indonesian Penal Code in Addressing Transnational Cybercrime

The information technology revolution has not only disrupted the social order but also fundamentally transformed the *modus operandi* of crimes. The emergence of contemporary criminal variants such as cybercrime, digital privacy exploitation, and mass disinformation (hoaxes) constitutes an anomalous phenomenon that evades the reach of the *Wetboek van Strafrecht* (the colonial-era Criminal Code). The obsolescence of this conventional instrument confirms the existence of a normative vacuum, urgently necessitating the reconstruction of the penal system. This regulatory reform is an absolute necessity to prevent the law from lagging behind the times; rather, it must engage in a responsive dialectic to guarantee legal certainty and public protection amidst the vortex of the digital era (Rahardjo, 2006).

Extraterritorial Jurisdiction in The New Indonesian Penal Code: Addressing Transnational Cybercrime

The transformation of technology based crime has dissolved local jurisdictional barriers, converting it into a transnational threat with highly complex dimensions. As an illustration, cyberattacks exploiting global network infrastructures frequently create an impasse for domestic authorities in tracking perpetrators and enforcing the law. Addressing this reality, the national penal system can no longer operate with an exclusively inward (internal) orientation; rather, it must absolutely integrate international cooperation instruments, primarily through extradition mechanisms and Mutual Legal Assistance (MLA) schemes. In response to this crucial urgency, the New Criminal Code formulates a legal breakthrough by expanding the spectrum of offense qualifications while simultaneously affirming extraterritorial jurisdiction to break the chain of impunity for perpetrators of cross-border digital crimes (Arief, 2017).

Furthermore, the transformation of cybercrime extends beyond mere novelties in its *modi operandi*, triggering a profound expansion in the typology of its perpetrators. The execution of such offenses is no longer dominated by individual actors; instead, it has shifted toward organized syndicate networks and even digital infiltrations orchestrated by state entities (state-sponsored cybercrime). These dynamics demand that the New Criminal Code be highly adaptive in calibrating proportionate penal sanctions and in constructing penal instruments that possess both preventive and repressive dimensions. However, at the implementation level, the codification of the National Criminal Code is considered to have fallen short of achieving absolute unification. Given that its enforcement continues to exhibit a heavy reliance on the ITE Law and other sectoral regulations, it is evident that Indonesia's penal landscape remains characterized by regulatory fragmentation (Aldriano, 2022).

The empirical acceleration of digital transformation has spawned social disruption, igniting acute juridical friction between the imperative of information control in cyberspace and the guarantee of freedom of expression. The escalating trend of prosecuting netizens for the dissemination of disinformation and offensive speech has sparked profound concerns regarding the threat of over-criminalization. Addressing this dilemma, the formulation of false news and hate speech offenses within the National Criminal Code necessitates a judicial interpretation approach anchored in the paradigm of progressive law. Such interpretative prudence is essential to ensure that criminal law enforcement does not mutate into an instrument of repression, but rather remains steadfastly aligned with the rule of law and the protection of human rights.

The reform of the penal system in Indonesia, manifested through the enactment of Law Number 1 of 2023 (the National Criminal Code), represents a milestone of decolonization after being shackled by the *Wetboek van Strafrecht* for over a century. This reform is not merely a textual replacement, but rather a paradigm leap aligned with the spirit of progressive law that shifts the punitive axis from a purely retributive nature toward a corrective approach and restorative justice. The manifestation of this shift is evident in the resolution of minor offenses, which now prioritizes the restoration of the victim's losses. Furthermore, this new codification architecture is designed to dialectically engage with the disruptions of the digital era. Although the handling of information technology offenses continues to position the ITE Law as *lex specialis*, the National Criminal Code has taken a progressive stride by incorporating and harmonizing the anatomy of cybercrime into the general criminal law system, thereby filling the normative void left unaddressed by classical criminal law (Muladi & Aief, 2022).

Confronted with these critical dynamics, the New Criminal Code introduces a legal breakthrough by expanding the spectrum of offense qualifications while affirming extraterritorial jurisdiction to break the chain of impunity for transnational digital offenders. Extraterritorial jurisdiction pertains to a state's legal capacity to exercise its sovereignty and authority beyond its territorial borders. At the implementation level, however, the application of this principle inevitably encounters several obstacles, particularly when intersecting with the jurisdictions of other sovereign states. In reality, the principle of extraterritorial jurisdiction may not be fully enforceable; a state inherently cannot exercise its coercive power within the territory of another nation, even if it holds legitimate jurisdiction over specific legal acts, subjects or objects of law, and legal interests (Rusdianto, 2023).

Efforts to disentangle the intricacies regarding the extent to which domestic courts possess the authority to adjudicate transnational offenses such as cybercrime have been facilitated by international law through six jurisdictional doctrines. This adjudicative authority can be established based on specific connecting factors. On the territorial dimension, a state may invoke the subjective territorial principle (focusing on the location where the crime is initiated) or the objective territorial principle (focusing on the location where the threatening impacts of the crime manifest). Concerning legal subjects, the active nationality principle grants a state the right to penalize its citizens who commit crimes abroad, whereas the passive nationality principle provides a substitutive right of prosecution to safeguard nationals who fall victim within foreign jurisdictions. Furthermore, for offenses targeting the essential security and existence of the state, the protective principle may be employed. Ultimately, the universality principle (universal interest jurisdiction) asserts that certain cyber offenses can be adjudicated by the jurisdiction of any state, effectively nullifying geographical and nationality barriers (Mukhsin, et al., 2023).

Addressing cybercrime via extraterritorial jurisdiction principles is essentially codified in Articles 4 through 8. The New Criminal Code marks a paradigm leap, extending the jurisdiction of Indonesian penal law beyond territorial boundaries much more explicitly than the colonial era *Wetboek van Strafrecht* (WvS). These provisions are outlined across several articles embodying the tenets of extraterritoriality. Article 4 (Protective/Passive Nationality Principle): Acting as the pivotal clause for cyber offenses, this article dictates that Indonesian penal law is applicable to anyone outside Indonesian borders who commits an act threatening national interests. Revolutionarily, Article 4(e) unequivocally lists 'information technology and electronic

transactions' among the protected interests of the state. Article 5 (Active Nationality / Personality Principle): This establishes that Indonesian penal law is binding upon Indonesian citizens. If a citizen perpetrates a cybercrime (such as online fraud) from a foreign country, they can still be prosecuted under Indonesian law. Article 6 (Universality Principle): This article extends Indonesian penal law to offenses committed outside its territory that are acknowledged as crimes by international law. Articles 7 and 8: These articles provide supplementary rules on the application of international law and specify exemptions from jurisdictional enforcement for certain entities.

This study concludes that the nature of the National Criminal Code reform particularly in responding to the digital ecosystem remains inherently transitional. Although the new codification has incorporated several information technology offenses, its regulatory framework is still confined to a normative textual approach; hence, it is deemed inadequate to untangle the anomalies of continuously evolving cybercrimes. Consequently, this reconfiguration of criminal law must be construed as an initial foundational stepping stone (a starting point) rather than a finalized legal product. The complexity of future challenges will pivot on the effectiveness of its implementation, which strictly necessitates synchronization with sectoral regulations (*lex specialis*). The absence of regulatory harmonization and institutional capacity reinforcement will ultimately reduce the significance of this reform to a mere symbolic legal monument, devoid of any progressive implications for the empirical operation of the criminal justice system (Fajriansyah, et al., 2025).

Substantively, the existence of the National Criminal Code represents the state's fundamental initiative to reconstruct the penal system, rendering it more adaptive and aligned with contemporary dynamics. Although this codification does not expressly incorporate the nomenclature of cybercrime or cyber offenses, the essence of several of its norms has implicitly accommodated enforcement instruments against various forms of unlawful acts materialized within the digital ecosystem.

In reality, the formulation of norms within the New Penal Code is excessively broad and falls short of addressing the technical anatomy of cyber offenses, including the exploitation of electronic systems, unlawful intrusions, malware distribution, and digital privacy breaches. This gap signifies that the absolute unification and criminalization of cybercrimes within the general criminal law framework remain unfulfilled. As a result, the enforcement against cyber offenses remains strictly anchored to *lex specialis* legislation, specifically the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law.

The complexity of cybercrime is tangibly manifested through its transnational nature, wherein the perpetrators, victim entities, and digital infrastructure bases may be dispersed across disparate sovereign jurisdictions. This borderless phenomenon imperatively demands the presence of penal instruments that are inherently elastic and collaborative, particularly concerning the resolution of jurisdictional conflicts, extradition, and mutual legal assistance schemes. Ironically, the architecture of the National Criminal Code is observed to still suffer from a normative vacuum in this regard; there is yet to be an explicit formulation designing the operational mechanisms for the enforcement of cross-border cybercrimes. In fact, the availability of regulations with an extraterritorial dimension is a juridical absolute required to respond to the globalization of legal systems and the global escalation of digital crime threats.

The existence of the National Criminal Code although it does not specifically formulate the procedural laws for extradition or Mutual Legal Assistance (MLA) plays a central role as a substantive prerequisite for the operationalization of these international instruments. This complementary relationship is manifested through three juridical constructions. First, the fulfillment of the dual criminality principle. The expansion of extraterritorial jurisdiction enshrined in Article 4 of the Criminal Code provides legitimacy for domestic law enforcement to submit extradition or MLA requests, considering that cyber offenses have now been unequivocally qualified within the national positive legal framework. Second, normative affirmation through Article 9 of the Criminal Code. This provision constructs a judicial bridge between national law and global agreements, asserting that the application of jurisdiction (Articles 2 through 8) shall not diminish the state's authority to execute the surrender of suspects to foreign jurisdictions. Third, doctrinal synchronization with international standards. This codification transformation philosophically affirms the spirit of global conventions, such as the Convention on Cybercrime (Budapest Convention), thereby ensuring that Indonesia's penal landscape is gradually harmonized with transnational parameters.

CONCLUSIONS

The rapid advancement of information technology in the digital era has fundamentally transformed the dynamics of transnational organized crime, leading to a massive and alarming escalation of cybercrime. Characterized by high perpetrator anonymity, automated operations, and the destructive ability to propagate simultaneous attacks across multiple jurisdictions, cybercrime inherently shatters the rigid territorial boundaries of conventional criminal law. Because perpetrators, victims, and digital infrastructures are frequently dispersed across completely different sovereign states, addressing this borderless threat necessitates a critical paradigm shift from traditional territorial principles toward extraterritorial jurisdiction. This global necessity for cooperative, cross-border legal frameworks is heavily underpinned by international instruments such as the 2001 Budapest Convention on Cybercrime.

In a strategic response to these complex global challenges and as an effort to decolonize its legal system from the Dutch-inherited *Wetboek van Strafrecht* (WvS), Indonesia enacted the New National Criminal Code (Law Number 1 of 2023). This

codification marks a progressive and humanistic milestone in the nation's penal reform, designed to be highly adaptive to contemporary technological disruptions. A revolutionary breakthrough within this new penal regime is the explicit expansion of extraterritorial jurisdiction, which is systematically codified in Articles 4 through 8. Most notably, Article 4(e) functions as a pivotal protective clause, firmly asserting that Indonesian penal law applies to any individual outside the country's borders who commits an act that threatens national interests specifically concerning information technology and electronic transactions.

Despite these significant progressive strides, the implementation of the New Penal Code remains inherently transitional and is accompanied by notable structural challenges. The formulation of its norms is considered excessively broad and lacks the specific technical anatomy required to comprehensively detail cyber offenses, such as complex system infiltrations or digital privacy breaches. Furthermore, the newly established legal architecture still suffers from a procedural vacuum; it lacks explicit operational mechanisms for executing cross-border enforcement, handling jurisdictional clashes, or processing extradition and Mutual Legal Assistance (MLA) specifically for cybercrimes. As a direct consequence of this regulatory fragmentation, the actual prosecution and enforcement of cyber offenses in Indonesia continue to rely heavily on *lex specialis* legislation, primarily the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law.

Ultimately, while the New Penal Code functions as an initial foundational stepping stone rather than a finalized, all-encompassing legal product, its substantive existence is absolutely vital for the future of international law enforcement. By unequivocally integrating the essence of cyber offenses into the general national legal framework, the code successfully fulfills the crucial principle of dual criminality. This integration provides domestic law enforcement with the necessary legal legitimacy to validly submit extradition and MLA requests to foreign jurisdictions. Supported by provisions that harmoniously bridge national law with global agreements, this reform ensures that Indonesia's penal landscape is gradually aligning with transnational parameters, provided it is followed by continuous regulatory synchronization and the strengthening of institutional capacities to combat global cybercrime syndicates effectively.

REFERENCES

- 1) Aldriano, M. A. (n.d.). Cyber Crime Dalam Sudut Pandang Hukum Pidana [Cyber Crime from the Perspective of Criminal Law]. Jurnal Kewarganegaraan 6 (1), 2169-2175.
<https://journal.upy.ac.id/index.php/pkn/article/download/2947/pdf/7209>
- 2) AllahRakha, N. 2024. Transformation of Crimes (Cybercrimes) in Digital Age. International Journal of Law and Policy 2 (2), 1–19.
<https://doi.org/10.59022/ijlp.156>
- 3) Amrani, H. 2019. Politik Pembaharuan Hukum Pidana [Politics of Criminal Law Reform]. UII Press.
- 4) Ardiansyah, M. R. and Edrisy, I. F. 2025. Tinjauan Pembaharuan Sistem Pemidanaan di Indonesia dalam KUHP Baru [Review of the Penal System Reform in Indonesia under the New Criminal Code]. Journal Evidence of Law 4 (3), 1641-1651.
- 5) Arief, B. N. 2017. Bunga Rampai Kebijakan Hukum Pidana [Anthology of Criminal Law Policy]. Kencana.
- 6) Arnel, P. and Faturoti, B. 2023. The Presecution of Cybercrime – Why Transnational and Extraterritorial Jurisdiction Should be Resisted. International Review of Law, Computers and Technology 37 (1), 29-51.
<https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2061888>
- 7) Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). 2024. Survey Penetrasi Internet Indonesia 2024 [Indonesian Internet Penetration Survey 2024]. <https://survei.apjii.or.id/survei>, 30.
- 8) Cahyono, S. T., Erni, W., and Hidayat, T. 2025. Reconstruction of Criminal Law Against Cybercrime in the Indonesia Criminal Justice System. DJH Dame Journal Hukum 1 (1), 111-133.
- 9) Council of Europe. 2001. Convention on Cybercrime. Europe Treaty Series No. 185.
- 10) Edrisy, I. F. 2019. Pengantar Hukum Siber [Introduction to Cyber Law]. Sai Wawai Publishing.
- 11) Fajriansyah, A., Siregar, R. A., and Panggabean, M. L. 2025. Criminal Law Reform In The Digital Era: An Analysis of The New Indonesian Penal Code. Jurnal Hukum Mimbar Justitia (JHMJ) 11 (1), 218-230.
<http://repository.uki.ac.id/20245/>
- 12) Government of Indonesia. 2008. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law Number 11 of 2008 concerning Electronic Information and Transactions].
- 13) Government of Indonesia. 2016. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law Number 19 of 2016 concerning Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions].
- 14) Government of Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [Law Number 27 of 2022 concerning Personal Data Protection].
- 15) Government of Indonesia. 2023. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana [Law Number 1 of 2023 concerning the Criminal Code].

- 16) Government of Indonesia. 2024. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions].
- 17) Gunawan, I. 2024. Teleconference Optimalization of Cross-Border Cybercrime Based on Extraterritorial Jurisdiction. *Jurnal Legal Reasoning* 7 (1), 30-47.
- 18) Khan, S. H., Zakir, M. H., Tayyap, A., and Ibrahim, S. 2024. The Role of International Law in Addressing Transnational Organized Crime. *Journal of Asian Development Studies* 13 (1), 283-294.
<https://poverty.com.pk/index.php/Journal/article/view/348>
- 19) Kusumaatmadja, M. and Agoes, E. R. 2003. Pengantar Hukum Internasional [Introduction to International Law]. Alumni.
- 20) Mukhsin, F. R., et al. 2023. The Review of Cybercrime Case Handling Based on Indonesian Jurisdiction And International Law. *International Journal of Law And Legal Ethics (IJLLE)* 4 (1), 23-35.
<https://ojs.udb.ac.id/IJLLE/article/view/2442>
- 21) Muladi and Arief, B. N. 2022. Bunga Rampai Kebijakan Hukum Pidana [Anthology of Criminal Law Policy]. Citra Aditya Bakti.
- 22) Rahardjo, S. 2006. Ilmu Hukum [Legal Science]. Citra Aditya Bakti.
- 23) Rusdianto. 2023. Application of Extraterritorial Jurisdiction Principles in Combating Cybercrime. *Mataram Journal of International Law* 1 (1), 2-24.
- 24) Situmeang, S. M. T. 2020. Cyber Law. Cakra.
- 25) Solikin, N. 2021. Pengantar Metodologi Penelitian Hukum [Introduction to Legal Research Methodology]. CV Penerbit Qiara Media.
- 26) Tuliakov, V. (n.d.). Transnational Criminal Law, Sovereignty and International Justice: Harmonization Challenges and Policy Evolution. *International Annals of Criminology* 36 (1), 383-405.
<https://www.cambridge.org/core/journals/international-annals-of-criminology/article/transnational-criminal-law-sovereignty-and-international-justice-harmonization-challenges-and-policy-evolution/F097A30BF6FC4906163BEFE3905D13B6>



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non-Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.