
The Implications of International Law for State Sovereignty in Handling Cross-Border Cybercrime

Yoan Barbara Runtunuwu

Universitas Negeri Manado

Email: yoanruntunuwu@unima.ac.id

Abstract

This research examines the implications of international law for state sovereignty in handling cross-border cybercrime, a phenomenon that increasingly challenges the territorially bounded assumptions underlying the traditional international legal order. The study aims to analyze how existing jurisdictional principles, the emerging concept of cyber sovereignty, and current international legal instruments interact in shaping states' capacity to investigate and prosecute cybercrime that spans multiple jurisdictions, while identifying the gaps that remain in reconciling sovereignty protection with effective cross-border enforcement. A qualitative approach is employed through normative legal research based on a literature study, drawing on primary legal materials such as international conventions and legal instruments, alongside secondary materials including scholarly books and journal articles, which are analyzed using statutory and conceptual approaches. The findings reveal that traditional jurisdictional principles are strained by the borderless character of cybercrime, that cyber sovereignty simultaneously protects and complicates cross-border cooperation, and that existing instruments such as the Budapest Convention and the Tallinn Manual 2.0 provide necessary but insufficient frameworks for reconciling these tensions. The study concludes that a more integrated, enforcement-oriented international legal framework is needed to balance sovereignty protection with the practical demands of prosecuting transnational digital crime.

Kata Kunci : *Implications, International Law, State Sovereignty, Handling Cross-Border, Cybercrime*

INTRODUCTION

The rapid expansion of global digital infrastructure has transformed cybercrime into one of the most pressing challenges for the international legal order, precisely because it rarely respects the territorial boundaries upon which the traditional system of state sovereignty is built. Public international law has historically organized itself around territorially bounded jurisdictions, yet cyberspace operates as a domain where conduct originating in one state can instantaneously produce harmful effects in another, unsettling long established assumptions about where state authority begins and ends (Kittichaisaree, 2017).

This tension has pushed scholars and policymakers to reconsider how classical

principles of jurisdiction, including territoriality, nationality, the protective principle, and universality, can be meaningfully applied to conduct that is inherently transnational. Cybercrime investigations frequently require access to data stored on servers located outside the prosecuting state, creating friction between the sovereign right of a state to control activity within its borders and the practical necessity of cross-border cooperation to gather evidence and apprehend offenders (Velasco, 2015).

International instruments such as the Budapest Convention on Cybercrime have attempted to bridge this gap by harmonizing domestic criminal law and establishing channels for mutual legal assistance, yet their reach remains limited by the voluntary nature of state accession and by significant non-participation from major



cyber powers. The search for a workable allocation of regulatory competence over online activity exposes a deeper dilemma, namely whether the future of internet governance lies in global legal harmonization or in a cyberspace that increasingly mirrors the fragmented borders of the offline world (Kohl, 2007).

At the same time, the concept of cyber sovereignty has emerged as states seek to reassert control over digital infrastructure and data flows within their territory, sometimes in tension with the borderless character of the crimes they are trying to combat. This dynamic has generated ongoing debate over how established principles such as non-intervention and the prohibition on the use of force under the UN Charter should apply to state and non-state cyber conduct, particularly given the persistent difficulties of attribution and enforcement in a decentralized digital environment (Chatinakrob, 2024).

Against this backdrop, this research examines the implications of international law for state sovereignty in the specific context of handling cross-border cybercrime. It situates the discussion within the broader literature on jurisdiction, sovereignty, and cyberspace governance, and asks how existing legal frameworks can be reconciled with the practical realities of prosecuting crimes that defy conventional territorial logic. This question carries particular weight for states seeking to protect national sovereignty while participating meaningfully in international cooperation mechanisms against transnational digital crime (Irawan et al., 2025).

Velasco (2015) traces the evolution of policies addressing cross-border access to computer data, analyzing European instruments on cybercrime jurisdiction and the role of internet service providers in facilitating law enforcement cooperation. The study concludes that existing jurisdictional models remain inadequate for the pace of technological change and proposes

alternative approaches for asserting prosecutorial authority over internet-related crime, though it stops short of connecting these jurisdictional mechanics to a broader theory of state sovereignty (Velasco, 2015).

Chatinakrob (2024) examines how information and communication technology threats challenge state sovereignty, focusing on sovereignty violations, extraterritorial effects, and the emerging paradigm of cyber sovereignty. The research analyzes the application of non-intervention and use of force principles to cyber operations and concludes that dedicated, cooperative international frameworks are essential given the limitations of existing instruments such as the Budapest Convention, though its treatment remains largely conceptual and state-to-state in orientation rather than focused on the operational handling of individual cybercrime cases (Chatinakrob, 2024).

Irawan et al. (2025) conduct a normative juridical study of criminal regulatory policy on cybercrime, with particular attention to threats against national sovereignty. The research maps the application of jurisdictional principles, including the nationality, protective, and universality principles, to cybercrime enforcement, and highlights universal jurisdiction as especially relevant for offenses with cross-border implications, while remaining largely descriptive of doctrine rather than offering an integrated enforcement-oriented framework (Irawan et al., 2025).

While the existing literature has extensively examined the theoretical tension between state sovereignty and the borderless nature of cyberspace, and while instruments such as the Budapest Convention and the Tallinn Manual 2.0 have been widely discussed as normative reference points, most prior studies remain confined either to doctrinal analysis of jurisdictional principles in isolation or to broad conceptual treatments of cyber sovereignty at the



level of state to state relations (Velasco, 2015; Chatinakrob, 2024; Irawan et al., 2025). There remains limited research that integrates these two strands, jurisdictional doctrine and sovereignty theory, into a unified analytical framework specifically oriented toward the practical implications for states handling cross-border cybercrime cases, particularly regarding how competing sovereign claims are, or should be, reconciled when enforcement actions in one state's cyberspace necessarily implicate the digital territory of another. This gap leaves an underexplored space regarding the concrete mechanisms through which international law can operationalize sovereignty protections without undermining the cooperative architecture needed to prosecute inherently transnational digital offenses.

This research offers novelty by moving beyond the largely separate treatments of jurisdictional doctrine and cyber sovereignty theory found in prior studies, instead constructing an integrated framework that examines the implications of international law for state sovereignty specifically as it plays out in the practical handling of cross-border cybercrime cases. Rather than treating sovereignty as a static, territorially fixed concept, this study approaches it as a contested and evolving construct that must be reinterpreted in light of the operational demands of cybercrime enforcement, including evidence gathering across borders, extradition, and multilateral cooperation, thereby contributing a more applied and enforcement-oriented perspective to a body of literature that has so far remained predominantly doctrinal or conceptual in orientation.

Cross-border cybercrime has become a routine feature of the digital economy, ranging from ransomware attacks that cripple hospital systems and critical infrastructure to large-scale data breaches, online fraud networks, and the trafficking of illicit content across multiple jurisdictions simultaneously. Criminal actors

exploit the fact that their operations can be planned in one country, executed through servers in a second, and targeted at victims in a third, all while leaving investigators to navigate a patchwork of national laws, evidentiary standards, and diplomatic sensitivities before a single suspect can even be identified, let alone prosecuted.

In practice, this means that law enforcement agencies are frequently forced to rely on slow and cumbersome mutual legal assistance treaties, informal cooperation between national cybercrime units, or the goodwill of private technology companies to obtain data stored abroad, often losing critical time in cases where evidence can be deleted or altered within hours. States, meanwhile, remain wary of ceding too much control over their digital territory to international bodies or foreign investigators, creating a persistent friction between the collective interest in effective cybercrime enforcement and each state's individual insistence on preserving its sovereign prerogatives over information and infrastructure within its borders.

METHOD

This research adopts a qualitative approach, which is considered appropriate given that the object under study concerns legal norms, principles, and doctrines rather than measurable numerical variables. A qualitative approach allows the researcher to explore in depth how international legal concepts and state sovereignty interact within the context of cross-border cybercrime, producing an interpretive and descriptive understanding rather than a statistical generalization (Creswell, 2014). This approach is particularly suited to legal research, where the primary task is to construct coherent argumentation from existing norms, principles, and doctrines rather than to test hypotheses through numerical measurement.



In terms of research type, this study is designed as normative legal research, also referred to as doctrinal legal research, which focuses on examining legal rules, principles, and the systematic relationships between legal norms as they apply to a given legal issue. Normative legal research is understood as a process of identifying legal principles and doctrines in order to provide a solution to a legal problem, making it the appropriate design for a study that seeks to assess the implications of international law for state sovereignty rather than to observe social behavior in the field (Marzuki, 2017). This type of research is further characterized by its reliance on the study of literature, including comparative legal analysis, legal principles, and legal systematics, without requiring direct field research (Soekanto & Mahmudji, 2015).

The data used in this research are entirely secondary data, obtained through a literature study (studi literatur) rather than through interviews, surveys, or direct field observation. These secondary data are classified into three categories, namely primary legal materials consisting of international conventions, treaties, and other binding legal instruments relevant to cybercrime and state sovereignty, secondary legal materials consisting of academic books, journal articles, and scholarly commentaries that explain and analyze those primary materials, and tertiary legal materials such as legal dictionaries and encyclopedic references used to clarify terminology and concepts (Marzuki, 2017). This tiered classification of legal materials ensures that the analysis remains grounded in authoritative sources while still benefiting from scholarly interpretation.

Data collection in this study is carried out through documentary and library-based techniques, in which relevant international instruments, academic literature, and journal articles are systematically identified, compiled, and reviewed. The literature study method involves searching, selecting, and examining written sources such as books, peer-reviewed articles, treaties, and institutional reports

that address the intersection of international law, sovereignty, and cybercrime, thereby allowing the researcher to synthesize existing scholarly discussions without direct interaction with human subjects (Creswell, 2014). This technique is considered efficient for legal research of this nature, as it enables comprehensive engagement with the accumulated body of knowledge on the topic while maintaining methodological rigor.

The collected data are analyzed using a qualitative descriptive analysis technique, in which legal materials are examined, categorized, and interpreted to identify patterns, relationships, and gaps in the existing literature before being synthesized into coherent legal argumentation. This process involves a statutory approach, which examines relevant international legal instruments, and a conceptual approach, which draws on legal principles and doctrines developed by scholars to construct an analytical framework for understanding the issue (Marzuki, 2017). Through this analytical process, the research moves from the identification of individual legal materials toward a broader synthesis that addresses the research question concerning the implications of international law for state sovereignty in handling cross-border cybercrime.

RESULT AND DISCUSSION

1. The Limits of Traditional Jurisdictional Principles in Addressing Cross-Border Cybercrime

The first finding of this research indicates that the classical principles of jurisdiction inherited from traditional international law, namely territoriality, nationality, the protective principle, and universality, struggle to provide a coherent basis for prosecuting cybercrime that by its very nature disregards physical borders. The territoriality principle, which historically served as the primary anchor of state jurisdiction, becomes analytically unstable when the locus delicti of a cyber offense may simultaneously involve the location of the perpetrator, the physical



location of the server used to commit the crime, and the location of the victim, each potentially situated in a different sovereign state (Kittichaisaree, 2017). This finding confirms the theoretical proposition that cyberspace, unlike the sea or airspace, is not a physical space subject to conventional international boundary law, making the extension of territorial jurisdiction to online conduct an inherently artificial exercise rather than a natural application of settled doctrine.

Building on this, the research finds that the nationality and protective principles offer only partial solutions, since they allow a state to claim jurisdiction based on the identity of the offender or victim, or on threats to national security and interests, but do not resolve the more fundamental problem of enforcement when the offender or evidence resides beyond the claiming state's physical reach. Irawan et al. (2025) similarly observe that while these principles remain doctrinally applicable to cybercrime, their practical utility is constrained by the absence of a corresponding enforcement mechanism capable of compelling cooperation from the state where the offender or data is actually located. This gap between jurisdictional claim and jurisdictional capacity represents a recurring theme in the data reviewed for this study, suggesting that the doctrine of jurisdiction, as conceived in a pre-digital era, was never designed to accommodate instantaneous, multi-territorial conduct of the kind cybercrime produces.

The principle of universality emerges from the findings as the most theoretically promising, yet practically underutilized, basis for jurisdiction over cybercrime. Traditionally reserved for offenses considered to affront the international community as a whole, such as piracy, genocide, and crimes against humanity, universal jurisdiction has been proposed by some scholars as a candidate framework for particularly severe cyber offenses whose transnational impact resembles these traditionally universal crimes. However, the extension of universal jurisdiction to cybercrime remains contested, both because cybercrime lacks the settled customary law status of the classical universal crimes and because

states remain reluctant to accept an expansive jurisdictional basis that could, in principle, be invoked against their own nationals or infrastructure by other states (Situmeang et al., 2026). This finding illustrates that the theoretical availability of a jurisdictional principle does not automatically translate into its practical acceptance by sovereign states protective of their own prerogatives.

Taken together, these findings support the argument, consistent with the regulatory competence theory advanced by Kohl (2007), that the persistence of location-centric jurisdictional rules in a borderless digital environment forces states into an uncomfortable choice between stretching traditional doctrine to the point of losing coherence, or accepting that cyberspace requires an entirely new jurisdictional paradigm. The data reviewed in this research suggest that most states have so far chosen the former path, applying traditional principles pragmatically and inconsistently on a case-by-case basis rather than committing to a unified doctrinal framework, a pattern that helps explain the persistent unpredictability and fragmentation observed in cross-border cybercrime enforcement.

2. Cyber Sovereignty and the Tension with International Cooperation Obligations

The second finding concerns the emergence of cyber sovereignty as a normative concept that states increasingly invoke to justify control over digital infrastructure, data flows, and online conduct occurring within, or affecting, their territory. This research finds that cyber sovereignty operates simultaneously as a shield and as a source of friction, in the sense that states rely on it to resist external interference in their domestic digital affairs, while the same principle, when asserted rigidly, can obstruct the very cross-border cooperation that effective cybercrime enforcement requires. Chatinakrob (2024) frames this as a paradigm in which cyberspace sovereignty extends traditional Westphalian notions of territorial control into the digital realm, yet without a corresponding international consensus on how far that control should extend when it intersects with the sovereign interests of other states.



This tension is further illuminated by the Tallinn Manual 2.0, which treats cyber infrastructure located within a state's territory as subject to that state's sovereignty, reinforcing the principle that unauthorized cyber operations against such infrastructure by another state may constitute a violation of sovereignty even in the absence of physical intrusion (Schmitt, 2017). The findings of this study indicate that this framing, while doctrinally significant, has ambiguous implications for cybercrime enforcement specifically, because it was developed primarily to address state-to-state cyber operations rather than criminal conduct by non-state actors, leaving a conceptual gap regarding how sovereignty protections should apply when a private criminal actor, rather than a foreign government, is the source of the intrusion.

A related finding is that the non-intervention principle, closely tied to sovereignty, creates additional complexity for cross-border cybercrime investigations that require one state's law enforcement agencies to access data or systems located in another state's territory. Even when such access is undertaken for legitimate investigative purposes, it risks being characterized as an intervention into the internal affairs of the state where the data resides unless conducted through recognized channels of cooperation, a concern that has grown more acute as states expand domestic legislation authorizing extraterritorial data access in the name of national security or crime prevention (Chatinakrob, 2024). This finding demonstrates that the protection of sovereignty and the practical necessities of cybercrime enforcement are not merely theoretically in tension but generate concrete legal risk for investigating states that overstep recognized cooperative frameworks.

These findings collectively suggest that cyber sovereignty, rather than resolving the jurisdictional uncertainties identified in the previous section, adds a further layer of normative contestation, since states must simultaneously defend their own digital sovereignty while seeking access to the sovereign digital space of others in order to investigate and

prosecute cybercrime effectively. This dynamic supports the broader theoretical observation that sovereignty in cyberspace functions less as a fixed legal boundary and more as a continuously negotiated claim, whose content and limits are shaped as much by state practice and diplomatic reciprocity as by settled international legal doctrine (Kittichaisaree, 2017).

3. The Adequacy of International Legal Instruments in Reconciling Sovereignty and Enforcement

The third finding relates to the capacity of existing international legal instruments, particularly the Budapest Convention on Cybercrime and its associated protocols, to reconcile the competing demands of state sovereignty and effective cross-border enforcement. The research finds that while the Budapest Convention represents the most comprehensive attempt to harmonize domestic criminal law and establish structured channels for mutual legal assistance and cross-border evidence access, its effectiveness is substantially limited by uneven ratification, with several major cyber powers remaining outside the treaty framework and therefore unbound by its cooperative obligations (Velasco, 2015). This finding indicates that even a well-designed multilateral instrument cannot fully resolve the sovereignty related enforcement gap when participation itself remains a matter of sovereign discretion.

Further analysis of the data reveals that mutual legal assistance treaties and other traditional cooperation mechanisms, while formally respectful of sovereignty because they require the consent of the requested state, are frequently too slow to match the evidentiary demands of cybercrime investigations, where digital evidence can be altered or destroyed within hours. Velasco (2015) highlights that the reliance on internet service providers as intermediaries in facilitating cross-border data requests has partially compensated for this procedural delay, yet this reliance introduces its own sovereignty concerns, since it effectively shifts elements of cross-border law enforcement cooperation away from formal state-to-state channels



and toward private commercial actors operating under the domestic law of a third jurisdiction.

The findings also point to the Tallinn Manual 2.0 as an influential but non-binding restatement of how existing international law, including sovereignty, due diligence, and jurisdiction, applies to cyber operations, which means it can guide state interpretation without imposing enforceable obligations capable of resolving concrete cybercrime cases (Schmitt, 2017). This soft law character, while valuable for clarifying contested doctrinal questions, means that states retain considerable latitude in deciding how to balance sovereignty protection against cooperative enforcement, resulting in inconsistent practice across different cybercrime cases and regions, a pattern also noted in the normative analysis of jurisdictional enforcement policy in Indonesia (Irawan et al., 2025).

Synthesizing these findings, this research concludes that current international legal instruments provide a necessary but insufficient foundation for reconciling state sovereignty with the practical demands of cross-border cybercrime enforcement, since they were largely designed either for narrower purposes, such as codifying substantive cybercrime offenses, or for interpretive guidance rather than binding multilateral obligation. This supports the broader argument advanced throughout the literature that the progressive development of dedicated, enforceable international legal frameworks, capable of directly addressing the intersection of sovereignty and cybercrime enforcement rather than treating each as a separate doctrinal concern, remains an unmet need in contemporary international law (Chatinakrob, 2024).

CONCLUSION

This research concludes that international law occupies an unsettled and continually contested position in relation to state sovereignty when it comes to handling cross-border cybercrime. The findings demonstrate that traditional jurisdictional principles, including territoriality, nationality, the protective principle, and universality, remain doctrinally applicable but are analytically strained when applied

to conduct that simultaneously implicates multiple territorial jurisdictions, leaving states to apply these principles pragmatically and inconsistently rather than through a unified framework. At the same time, the emergence of cyber sovereignty as a normative claim has added a further layer of complexity, since states rely on it both to protect their digital infrastructure from external interference and, paradoxically, to resist the very cross-border cooperation that effective cybercrime enforcement requires, a tension that existing instruments such as the Budapest Convention and the Tallinn Manual 2.0 have only partially addressed.

These conclusions carry the implication that the current international legal architecture, while providing a meaningful doctrinal foundation, has not yet evolved into a framework capable of fully reconciling the protection of state sovereignty with the operational demands of prosecuting inherently transnational digital offenses. Addressing this shortfall will likely require the progressive development of more binding and enforcement-oriented multilateral instruments, broader participation from states currently outside existing cybercrime conventions, and clearer doctrinal guidance on how sovereignty and cooperation obligations should be balanced in concrete enforcement scenarios. Future research would benefit from examining how specific regional cooperation mechanisms or bilateral arrangements have attempted to bridge this gap in practice, offering a more empirically grounded complement to the normative analysis undertaken in this study.

REFERENCES

Chatinakrob, T. (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), 25–50.



- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Irawan, B., Mulyanti, D., Budiaman, H., Rahman, Y. M., & Taufiqurrohman, A. (2025). Perspective of state sovereignty in law enforcement related to cyberlaw jurisdiction. *Law Reform*, 21(1), 120–134.
- Kittichaisaree, K. (2017). *Public international law of cyberspace*. Springer International Publishing.
- Kohl, U. (2007). *Jurisdiction and the internet: A study of regulatory competence over online activity*. Cambridge University Press.
- Marzuki, P. M. (2017). *Penelitian hukum* (Rev. ed.). Kencana.
- Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.
- Situmeang, S. M. T., Kamilia, E. R., Lutfiyah, N., & Aurora, D. M. (2026). Enforcement of the universality principle in combating cybercrime as a transnational crime. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, 16(1), 70–88.
- Soekanto, S., & Mahmudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat*. Raja Grafindo Persada.
- Velasco, C. (2015). Cybercrime jurisdiction: Past, present and future. *ERA Forum*, 16(3), 331–347.

