Science of Law
Vol. 2026, No. 10, 1-8, 2026
ISSN(E) 2995-8717
DOI: 10.55220/2995-8717.v2026i10.3341
© 2026 by the authors; licensee Scientific Hub

National Sovereignty in Cyberspace: Theoretical Foundations, the International Legal Framework, and Vietnam's Legal Practice

Pham Thanh Nga[1] ✉
Dau Cong Hiep[2]

[1]*Hanoi Department of Justice, Vietnam.*
[2]*Law Clinic, Hanoi Law University, Vietnam.*
(✉ Corresponding Author)

Abstract

This article examines the legal regime of national sovereignty in cyberspace from three perspectives: legal theory, public international law, and Vietnamese domestic law. Using doctrinal analysis, comparative analysis of state positions, and synthesis of state practice, it advances four findings. First, sovereignty is not excluded from cyberspace; it operates through the control that states exercise over the infrastructure, persons, and activities located on their territory. Second, the international community has reached consensus that existing international law, including sovereignty, applies in cyberspace, yet states remain deeply divided over whether sovereignty is a stand-alone rule of international law or merely a foundational principle. Third, jurisdiction, the principle of non-intervention, due diligence, state responsibility, and the prohibition of the use of force together form the core framework governing state conduct in cyberspace. Fourth, Vietnam's 2025 Law on Cybersecurity, equips the state with a fairly complete set of legal instruments to protect sovereignty, but it should be complemented by an official national position on the application of international law and by mechanisms that balance sovereignty, digital economic development, and human rights. The article concludes with policy and legislative recommendations, and argues that sovereignty should be treated as a rule with substantive content and a carefully calibrated violation threshold.

Keywords: Fact, International Law, Solution, State sovereignty, cyberspace, Vietnam.

1. Introduction

Within a few decades, cyberspace has moved from a technical environment to an essential infrastructure of national life. State administration, finance, energy, health care, transport, and national defense all run on information systems. In parallel, cyberattacks on critical infrastructure, cyber espionage, and information-manipulation campaigns conducted by states or by actors they support have become a routine feature of international relations. Episodes such as the denial-of-service attacks on Estonia in 2007, the Stuxnet worm of 2010, and the NotPetya attack of 2017 raise a core question: what rights do states hold, what obligations do they bear, and which legal instruments may they invoke in an environment where traditional geographic boundaries appear to blur?

The question is not merely academic. Sovereignty is the foundation of the entire modern international legal order. If sovereignty does not apply in cyberspace, or applies only weakly, the mechanisms that protect states against external interference lack a firm legal basis. Conversely, if sovereignty is construed too broadly, it can become a justification for fragmenting the global network, restricting information flows, and infringing human rights. The relevance of the topic therefore lies in the need to determine, rigorously, the legal boundaries of sovereignty in cyberspace.

For Vietnam the topic carries particular practical significance. On 10 December 2025 the 15th National Assembly adopted Law on Cybersecurity No. 116/2025/QH15, which takes effect on 1 July 2026 and replaces both the 2018 Law on Cybersecurity and the 2015 Law on Network Information Security. The consolidation of the domestic framework coincides with major developments at the international level, from the United Nations process on responsible state behavior in cyberspace to the opening for signature, in Hanoi, of the United Nations Convention against Cybercrime. Placing domestic law in relation to international law is therefore unavoidable.

The article addresses three questions. (1) How is state sovereignty understood and applied in cyberspace under existing international law? (2) What are the principal disagreements among states and scholars, and which approach is more persuasive? (3) What has Vietnamese law already done to give effect to sovereignty in cyberspace, and what must be improved to align protection of sovereignty with Vietnam's international commitments?

The article makes three contributions. It integrates the theoretical, international, and domestic dimensions, which the literature usually treats separately. It offers a reasoned assessment of the "rule versus principle" debate that pairs a substantive position with a calibrated violation threshold. And it identifies a concrete gap in Vietnam's

© 2026 by the authors; licensee Scientific Hub

external legal posture, namely the absence of a comprehensive official statement on how international law applies to cyber operations, and links that gap to specific, actionable recommendations.

2. Methodology and Sources

The study is doctrinal and qualitative. It combines three methods. First, normative analysis is applied to the recognized sources of international law, namely treaties, customary international law, the case law of international courts and tribunals, and United Nations instruments, following the framework of Article 38 of the Statute of the International Court of Justice. Second, comparative analysis is used to compare the publicly stated positions of states on the application of international law in cyberspace, including those of the United Kingdom, the United States, France, Germany, the Netherlands, the African Union, and the group of states emphasizing "cyber sovereignty." Third, synthesis is used to draw conclusions and to formulate recommendations for Vietnam.

The primary materials comprise judgments and awards (*Island of Palmas*, *Lotus*, *Corfu Channel*, *Trail Smelter*, *Nicaragua*, *Pulp Mills*), reports of the United Nations Groups of Governmental Experts (GGE) and Open-Ended Working Group (OEWG), the *Tallinn Manual 2.0*, the International Law Commission's Articles on State Responsibility, and Vietnamese legal instruments. The secondary materials are leading monographs and journal articles on cyber sovereignty, due diligence, cyber espionage, and the use of force.

Two caveats frame the analysis. First, the reports of the GGE and OEWG are not treaties and their norms are voluntary; they are treated here as evidence of state practice and *opinio juris* rather than as sources of binding obligations. Second, the *Tallinn Manual 2.0* is the work of an independent group of experts and has no binding force; it is used as a systematic reference point, not as authority in itself. Vietnamese official documents were consulted as they were publicly available to the author, and statements about Vietnam's official positions are limited accordingly.

3. Theoretical Foundations of Sovereignty in Cyberspace

3.1. A Legal "Zone" or a Layer of Infrastructure?

How one understands the legal nature of cyberspace determines how sovereignty applies to it. In the early period of the commercial Internet, an influential school held that cyberspace was a "place" separate from physical territory and therefore required its own rules, produced by the community of users (Johnson & Post, 1996). The 1996 Declaration of the Independence of Cyberspace was the most extreme expression of this idea, proclaiming that governments have no sovereignty where users gather (Barlow, 1996). Two decades of practice have refuted the claim. Goldsmith and Wu (2006) showed that states have used coercive power over intermediaries, infrastructure providers, and users located within their territory to impose their laws on the Internet, undermining the illusion of a "borderless" space. Lessig (1999) argued that code and technical architecture are themselves instruments of regulation that states and private actors can shape, rather than a zone immune from law.

The approach now widely accepted is the layered model. On this view cyberspace comprises three layers: a physical layer (servers, fiber-optic cables, exchange points, end-user devices), a logical layer (protocols, software, applications, data), and a social layer (users, organizations, and the relationships they establish) (Schmitt, 2017). The legally salient point is that the physical layer and a substantial part of the logical layer are always located on the territory of one or more states, and the persons who operate them are always subject to the jurisdiction of some state. Cyberspace is therefore not an area beyond sovereignty, as the high seas or outer space are; it is an operational environment superimposed on sovereign territories. This conclusion is the starting point of most contemporary scholarship and policy instruments.

3.2. The Content of Sovereignty in International Law

In the classic *Island of Palmas* arbitration, Judge Max Huber defined sovereignty in relations between states as independence, that is, the right to exercise the functions of a state in a portion of the globe to the exclusion of any other state (*Island of Palmas Case*, 1928). The 1933 Montevideo Convention lists a defined territory, a permanent population, a government, and the capacity to enter into relations with other states as the attributes of statehood (Convention on Rights and Duties of States, 1933). The Charter of the United Nations gives sovereignty operational form through the principle of sovereign equality (Article 2(1)), the prohibition of the threat or use of force against the territorial integrity or political independence of any state (Article 2(4)), and the protection of matters essentially within domestic jurisdiction (Article 2(7)) (Charter of the United Nations, 1945).

Doctrine commonly distinguishes two faces of sovereignty. Internal sovereignty is the supreme authority of the state over the territory, persons, property, and activities within it, including legislative, executive, and judicial power. External sovereignty is autonomy in international relations and the right not to be interfered with or dominated by other states. In *Lotus*, the Permanent Court of International Justice stated a basic rule: the first and foremost restriction that international law imposes on a state is that it may not exercise its power in any form in the territory of another state unless a permissive rule allows it (*S.S. "Lotus"*, 1927). In *Nicaragua*, the International Court of Justice (ICJ) affirmed that territorial sovereignty and political independence are protected by customary law and are closely bound up with the prohibitions of force and intervention (*Military and Paramilitary Activities in and against Nicaragua*, 1986).

From these sources three legal components of sovereignty relevant to cyberspace can be distilled: (a) supreme authority over infrastructure, persons, and activities within the territory; (b) the inviolability of territory and of state functions against the conduct of other states; and (c) autonomy in deciding matters within domestic jurisdiction without external coercion.

3.3. From "Anarchic Freedom" to "Controlled Sovereignty"

Tsagourias (2015) observed that the debate on the legal status of cyberspace has shifted from the question of *whether* sovereignty applies to the question of *how and to what extent* it applies. This shift reflects two concurrent trends. On the one hand, most states accept that they hold authority over information infrastructure located on

© 2026 by the authors; licensee Scientific Hub

their territory and may regulate related activities. On the other hand, because data flows cross borders and systems overlap, identifying a connecting factor sufficient for a state to exercise jurisdiction, and determining what conduct infringes another state's sovereignty, are legally complex problems. The following sections address these problems.

4. The International Legal Framework on Sovereignty in Cyberspace

4.1. A Fragmented Set of Sources

No global treaty comprehensively governs state conduct in cyberspace. The legal regime of sovereignty is therefore assembled from three layers of sources: (i) general international law (the UN Charter, customary international law, general principles of law, and judicial decisions); (ii) "soft law" policy instruments of the United Nations, above all the reports of the GGE and the OEWG; and (iii) specialized treaties, whether regional or thematic, such as the conventions on cybercrime. The international community's approach has been to apply existing law to the new environment rather than to negotiate immediately a dedicated "cyber sovereignty treaty."

4.2. The United Nations Process

The 2013 report of the Group of Governmental Experts was a turning point. For the first time, states, including major cyber powers, agreed that international law, and in particular the UN Charter, applies to cyberspace, and that state sovereignty and the norms and principles deriving from it apply to state conduct in information and communications technologies (ICTs) and to state jurisdiction over ICT infrastructure within their territory (UN General Assembly, 2013).

The 2015 report developed two further strands. First, it stated that states must observe sovereignty, sovereign equality, the peaceful settlement of disputes, and non-intervention in the internal affairs of other states when using ICTs. Second, it set out voluntary norms of responsible behavior, including the norm that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (UN General Assembly, 2015). This norm mirrors, in recommendatory form, the customary duty of due diligence analyzed in Section 6. The General Assembly welcomed the report and called on states to be guided by it in their use of ICTs.

The 2021 GGE report further clarified the implementation of the norms and added commentary on how each should be understood, while reaffirming that existing international law applies and should be better understood through discussion among states (UN General Assembly, 2021a). In parallel, the 2019–2021 Open-Ended Working Group, established by the General Assembly and open to all member states, adopted its final report by consensus, reaffirming the GGE conclusions and recognizing the need for continued discussion of how international law applies (UN General Assembly, 2021b). The 2021–2025 OEWG concluded in July 2025 with the adoption of a final report and agreement to establish a permanent global mechanism on security in the use of ICTs (UN OEWG, 2025).

The legal character of these instruments must be kept in view. GGE and OEWG reports are not treaties, and the norms they contain are voluntary and non-binding. However, their affirmation that existing international law applies reflects state consensus and has evidentiary value as state practice and *opinio juris* in the formation and confirmation of customary international law (Finnemore & Hollis, 2016). Thus, even though they create no new obligations, these instruments strengthen the proposition that sovereignty is a legal concept operative in cyberspace.

4.3. The Role of the Tallinn Manual 2.0

The *Tallinn Manual 2.0*, prepared by an independent group of international experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence, is the most systematic effort to codify the international law applicable to cyber operations in peacetime. It is not binding, but it is widely cited in state practice and scholarship. Rule 1 provides that the principle of state sovereignty applies in cyberspace; Rules 2 and 3 distinguish internal and external sovereignty; and Rule 4 provides that a state must not conduct cyber operations that violate the sovereignty of another state (Schmitt, 2017). On this approach, a state exercises sovereignty over cyber infrastructure, persons, and cyber activities on its territory, even where the infrastructure is privately owned.

Notably, the *Manual* records that the group of experts agreed on two situations that certainly constitute a violation of sovereignty: a cyber-operation causing physical damage or loss of functionality of infrastructure, and a cyber-operation interfering with or usurping inherently governmental functions. For "gray zone" situations, such as rendering infrastructure non-functional without physical damage, or penetrating systems to collect information, the experts could not reach consensus on whether a violation occurs (Schmitt, 2017). This lack of consensus is the premise of the debate analyzed next.

5. Discussion

The central issue in the legal regime of sovereignty in cyberspace is whether sovereignty by itself creates an independent binding obligation (a rule), or is only a foundational principle underlying other, specific rules such as the prohibitions of the use of force and of intervention (a principle). The consequences differ. If sovereignty is a rule, a state's cyber operation may constitute an internationally wrongful act even if it does not reach the threshold of the use of force or coercive intervention. If sovereignty is only a principle, lower-threshold activities, such as system penetration, espionage, or moderately disruptive campaigns, are not unlawful under international law unless they satisfy the conditions of another rule.

Corn and Taylor (2017) are the most prominent defenders of this view. They argue that positive international law contains no separate rule prohibiting every cross-border act merely because it intrudes on sovereignty; sovereignty is a foundational principle given concrete expression in clear rules (the prohibitions of force and intervention), and state practice in areas such as espionage and intelligence activity shows no general prohibition of such activities. A pragmatic argument accompanies this: an overly broad sovereignty rule would make most information-gathering and active-defense activity unlawful and thereby constrain states' capacity to respond.

© 2026 by the authors; licensee Scientific Hub

This view is reflected in the position of the United Kingdom, whose Attorney General, Jeremy Wright, stated in 2018 that the United Kingdom does not consider the concept of sovereignty alone to provide a sufficiently clear basis for extending a specific prohibition on cyber interference beyond the scope already governed by the principle of non-intervention (Wright, 2018). The United States, through the remarks of the Department of Defense General Counsel in 2020, likewise expressed caution, stating that it was not certain that state practice has established a distinct rule of sovereignty beyond existing rules (Ney, 2020). This position should be read against the earlier U.S. government approach, which had already affirmed that international law applies to cyberspace generally (Koh, 2012).

The opposing view has been systematically defended by Schmitt and Vihul (2017). They point out that sovereignty has long been the source of specific obligations (such as the prohibition of exercising authority on another state's territory or of unauthorized entry into its airspace or territorial sea), that state practice and case law treat these as independent violations, and that without this rule, harmful cyber operations falling below the threshold of coercive intervention would lie outside the regulation of international law, creating a dangerous legal gap.

Several states have declared support for this understanding. In 2019 France stated that any unauthorized penetration of French systems by a state, as well as any effects produced on French territory by digital means, may constitute a violation of sovereignty (République française, 2019). In 2021 Germany recognized sovereignty as a rule of international law that cyber operations with effects on its territory can violate (Federal Government of Germany, 2021). In 2019 the Netherlands likewise treated respect for sovereignty as an independent rule and considered that remote intrusion into computer systems in the Netherlands may constitute a violation depending on its degree (Government of the Netherlands, 2019). The African Union's Common Position, adopted in 2024, also affirms sovereignty as a foundational principle that ICT activities can violate (African Union Peace and Security Council, 2024). After surveying state practice and doctrine, Delerue (2020) concluded that support for sovereignty as a rule has the stronger basis, although the limits of its application remain open.

5.1. States Emphasizing "Cyber Sovereignty"

Beside this scholarly debate there is a policy-oriented approach, emphasized by China, the Russian Federation, and several other members of the Shanghai Cooperation Organisation, commonly called "cyber sovereignty." At the Second World Internet Conference in 2015, President Xi Jinping proposed respect for cyber sovereignty as a foundational principle of Internet governance, including each country's right to choose its own path of development and model of network regulation (Xi, 2015). The International Code of Conduct for Information Security, submitted by these states to the United Nations in 2015, refers to states' rights over Internet-related public policy and to the duty to refrain from using ICTs to interfere in internal affairs (China et al., 2015). China's 2017 International Strategy of Cooperation on Cyberspace stresses similar points (Ministry of Foreign Affairs of the PRC & Cyberspace Administration of China, 2017). At the domestic level, the Russian Federation enacted its "sovereign Internet" law in 2019, enabling authorities to increase control over routing infrastructure and, in certain circumstances, to isolate the national network from the global network (Russian Federation, 2019).

Two layers of meaning should be distinguished. At the first, "cyber sovereignty" restates the widely accepted principle of sovereignty, consistent with the GGE reports. At the second, it can serve to justify expansive controls over content and information flows that may collide with human rights obligations. Some Western states criticize this second layer and favor multistakeholder governance and an open Internet. The division here concerns policy values more than any principle of international law.

5.2. Assessment

In the author's view, the position that sovereignty is a rule is more persuasive, for three reasons. First, in terms of legal history, territorial sovereignty has always been treated by practice and case law as the source of specific obligations that the ICJ has applied, such as the principle that a state must respect the sovereignty of others and may not use its territory contrary to their rights (*Corfu Channel Case*, 1949). Second, functionally, recognizing the rule fills the gap between wholly lawful conduct and conduct reaching the threshold of force or coercive intervention, the "gray zone" in which most hostile cyber activity occurs. Third, the growing number of states publicly supporting the rule constitutes a practice trend that is significant for the formation of custom.

However, this approach is reasonable only if accompanied by a carefully defined violation threshold. Consistent with the *Tallinn Manual*, the threshold should rest on criteria of effect (physical damage or significant loss of infrastructure functionality) and of interference with inherently governmental functions, rather than treating every unauthorized access as a violation (Schmitt, 2017). Such a threshold both protects states and avoids turning sovereignty into an instrument that obstructs even lawful defensive activity. The result is a rule with content rather than a slogan.

5.3. Specific Legal Consequences of Sovereignty in Cyberspace

Jurisdiction over infrastructure, persons, and cyber activities

The first consequence of internal sovereignty is jurisdiction. According to the *Tallinn Manual 2.0*, a state has authority over cyber infrastructure, persons, and cyber activities on its territory, including legislative authority (regulation of infrastructure, data, and services), executive authority (supervision, inspection, enforcement), and judicial authority (Schmitt, 2017). Beyond the territorial basis, a state may invoke other bases recognized in international law, such as the nationality of the actor, effects occurring on its territory (the effects principle), the protection of core security interests, and, in some cases, universal jurisdiction. The Budapest Convention on Cybercrime of 2001 illustrates how states have designed bases of jurisdiction over cybercrime by reference to territory and nationality (Convention on Cybercrime, 2001, art. 22).

The greatest challenge lies in extraterritorial jurisdiction over data stored abroad. The U.S. CLOUD Act of 2018 allows U.S. law enforcement to compel providers subject to U.S. jurisdiction to disclose data located abroad if it is within the provider's "possession, custody, or control" (Clarifying Lawful Overseas Use of Data Act, 2018).

© 2026 by the authors; licensee Scientific Hub

This provision is controversial for the boundary it draws between lawful law enforcement and infringement of the data sovereignty of the state where the data is stored. Kohl (2017) and her co-authors show that states increasingly tend to extend their jurisdiction in overlapping ways, producing conflicts of jurisdiction and a need for stronger international coordination. The general principle of international law is that a state may not perform enforcement acts on another state's territory without consent (*S.S. "Lotus"*, 1927), but it may prescribe rules with extraterritorial effect where there is a reasonable and substantial connection.

5.4. The Principle of Non-Intervention

The principle of non-intervention protects each state's right to decide matters within its domestic jurisdiction free from external coercion. In *Nicaragua*, the ICJ identified two elements: (i) the act bears on matters in which a state is entitled to decide freely (such as the choice of political, economic, social, and cultural system and of foreign policy), and (ii) the act is coercive in nature (*Military and Paramilitary Activities in and against Nicaragua*, 1986). The *Tallinn Manual 2.0* applies this to cyberspace: a cyber-operation can constitute unlawful intervention where it coerces another state on a matter of internal sovereignty, for example by coercive interference in an electoral system or by paralyzing government agencies to force a change of policy (Schmitt, 2017).

The difficulty is that coercion is generally understood to require a sufficient degree of seriousness. Information-manipulation campaigns do not use compulsion; they aim to influence the perceptions of the population and often struggle to meet this condition, prompting debate over whether to broaden the concept of coercion or to treat such conduct as a violation of sovereignty more generally. This illustrates that an independent sovereignty rule complements the principle of non-intervention rather than replacing it.

5.5. The Duty of Due Diligence

The ICJ's *Corfu Channel* judgment established that every state has an obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states (*Corfu Channel Case*, 1949). The *Trail Smelter* arbitral award set out a similar principle in the environmental field, and the ICJ confirmed the duty of due diligence in *Pulp Mills* (*Trail Smelter Case*, 1941; *Pulp Mills on the River Uruguay*, 2010). In the cyber context, Rule 6 of the *Tallinn Manual 2.0* holds that a state must exercise due diligence in not allowing its territory to be used for cyber operations that affect the rights of other states and produce serious adverse consequences (Schmitt, 2017). Norm 13(c) of the 2015 GGE report was framed in this spirit, albeit as a voluntary recommendation (UN General Assembly, 2015).

Scholars disagree on the status of this duty. Jensen and Watts (2017) warn that, if applied rigidly, a cyber-due diligence duty would place too heavy a burden on states with limited capacity and could be abused to justify broad surveillance. A reasonable approach is to treat it as an obligation of conduct, not of result: states are required to take reasonable measures within their capacity once they have actual or constructive knowledge of harmful activity. For developing states such as Vietnam, this implies building incident-response capacity and international cooperation, rather than bearing responsibility for every activity originating from infrastructure on their territory.

5.6. State Responsibility and Countermeasures

The general conditions for state responsibility are that conduct is attributable to the state and breaches that state's international obligation, under the International Law Commission's 2001 Articles on State Responsibility (International Law Commission, 2001). The conduct of state organs is automatically attributed to the state; the conduct of individuals or groups is attributable only if they act under the state's direction or control (Article 8). In cyberspace the salient difficulty is attribution, because attackers conceal their identity and use third-party infrastructure and proxy groups. International law prescribes no fixed standard of proof, but a state invoking responsibility needs reasonably sufficient evidence.

When a state is the victim of an internationally wrongful act, it may adopt countermeasures to induce the responsible state to cease the conduct and make reparation, subject to conditions of proportionality, notification, and reversibility (International Law Commission, 2001, arts. 49–54). Countermeasures are lawful only in response to a breach of international law. It is here that the view of sovereignty as a rule yields practical benefit: it widens the range of conduct classified as wrongful, giving victim states a further legal basis for responding below the level of force.

5.7. Prohibition of the Use of Force and Self-Defense

Article 2(4) of the Charter prohibits the threat or use of force against the territorial integrity or political independence of any state, and Article 51 preserves the right of self-defense in the event of an armed attack (Charter of the United Nations, 1945). According to the ICJ, distinguishing an "armed attack" from less grave forms of the use of force depends on scale and effects (*Military and Paramilitary Activities in and against Nicaragua*, 1986). Roscini (2014) argues that a cyber-operation can constitute a use of force when its consequences are comparable to those of conventional force, such as serious physical damage or casualties. This threshold is very high relative to most cyber operations. At the level of sovereignty, therefore, most disputes in substance lie below the threshold, which reinforces the importance of the rules on sovereignty and non-intervention.

5.8. Cyber Espionage and Sovereignty

Espionage is the most sensitive area. International law contains no general rule prohibiting espionage, and state practice shows that most states conduct intelligence activities. Nevertheless, Buchan (2018) argues that cyber espionage carried out by remote intrusion into another state's systems may violate sovereignty where it amounts to an unauthorized exercise of power on another state's territory, even without physical presence. States that support the sovereignty rule tend to regard intrusion for espionage purposes as capable of violating sovereignty depending on circumstances, while others maintain that espionage is not prohibited by international law as a general rule. This disagreement shows that the legal regime of sovereignty in cyberspace is still taking shape.

© 2026 by the authors; licensee Scientific Hub

5.9. Sovereignty and Human Rights

Finally, sovereignty is not absolute. State activity within the territory is always limited by international obligations, including human rights obligations. The International Covenant on Civil and Political Rights (ICCPR) protects privacy (Article 17) and freedom of expression, including the freedom to seek, receive, and impart information through any medium (Article 19), and permits restrictions on expression only where provided by law and necessary for national security, public order, or other legitimate aims (International Covenant on Civil and Political Rights, 1966). Hence, when a state invokes sovereignty to block or remove content or to require data storage, these measures must satisfy the requirements of legality, necessity, and proportionality. This is the key point that distinguishes the legitimate exercise of sovereignty from the abuse of the concept.

5.10. Vietnam's Legal Framework for Protecting Sovereignty in Cyberspace

5.10.1. Constitutional And Political-Legal Foundations

The 2013 Constitution (as amended in part in 2025) declares in Article 1 that the Socialist Republic of Viet Nam is an independent, sovereign, unified country with territorial integrity, including its mainland, islands, sea, and airspace (Constitution of the Socialist Republic of Viet Nam, 2013). The Constitution does not list "cyberspace" as a separate part of the territory, which is consistent with the international view that cyberspace is not a new territorial "zone" but an operational environment tied to infrastructure and persons within the territory. Sovereignty in cyberspace is therefore protected through sovereignty over infrastructure, data, and activities located within Vietnam's territory and under its jurisdiction.

At the policy level, Politburo Resolution No. 29-NQ/TW of 25 July 2018 on the Strategy for Defending the Fatherland in Cyberspace and Resolution No. 30-NQ/TW of the same date on the National Cybersecurity Strategy oriented the protection of national sovereignty and interests in cyberspace as part of the cause of defending the Fatherland (Politburo, 2018a, 2018b). These documents provide the political foundation for the specialized legal system.

5.11. The Law on Cybersecurity Of 2025

Law on Cybersecurity No. 116/2025/QH15 comprises eight chapters and 45 articles, was adopted by the National Assembly on 10 December 2025, and takes effect on 1 July 2026. Under Article 44, from that date Law on Network Information Security No. 86/2015/QH13 (as amended by Law No. 35/2018/QH14) and Law on Cybersecurity No. 24/2018/QH14 cease to be effective (National Assembly, 2025a). The consolidation of the two laws aims to remove overlap, unify the management focal point, and improve risk governance. According to official dissemination materials, the new law also adds provisions on the responsibilities of enterprises providing services on telecommunications networks, the Internet, and value-added services to cooperate in preventing and removing information that violates cybersecurity upon request by competent authorities, together with new provisions on the use of technologies such as artificial intelligence for fraud and impersonation.

From the standpoint of sovereignty, three principal groups of legal instruments can be identified. The first is instruments for managing infrastructure and important information systems: the determination, appraisal, and security supervision of information systems important to national security, corresponding to the state's authority over infrastructure on its territory. The second is data management instruments: rules on storing user data in Vietnam and on the presence requirements for foreign enterprises, which were introduced in the 2018 Law on Cybersecurity and elaborated in Decree No. 53/2022/ND-CP, and are now carried forward and adjusted in the new law (National Assembly, 2018; Government of Viet Nam, 2022). The third is instruments for handling information and violations: mechanisms for requesting the removal of information, enterprise cooperation, and administrative and criminal sanctions.

On criminal jurisdiction, the 2015 Penal Code (amended in 2017) provides for effect over crimes committed within the territory (Article 5) and outside it (Article 6), and defines a group of crimes in the field of information technology and telecommunications networks in Chapter XXI (Articles 285 to 294) (National Assembly, 2015). This combination of territorial and extraterritorial bases is consistent with the international bases of jurisdiction analyzed in Section 6, and facilitates judicial cooperation in handling cybercrime.

5.12. Data Sovereignty

Together with the Law on Cybersecurity, the Law on Digital Data No. 60/2024/QH15 and the Law on Personal Data Protection No. 91/2025/QH15 form new pillars of data governance, reflecting a trend of treating data as a strategic resource and an object of national sovereignty (National Assembly, 2024, 2025b). From an international law perspective, data localization requirements and restrictions on cross-border data transfers are measures exercising legislative jurisdiction over actors with a substantial connection to the territory. In principle, such measures do not contravene general international law if there is a reasonable connection and they are applied without discrimination. However, they may be subject to international trade commitments (such as the electronic commerce and data flow commitments in free trade agreements) and to privacy obligations, and should therefore be designed to balance interests.

5.13. Vietnam in the International Process

Multilaterally, Vietnam is an active member of the United Nations and ASEAN. Within ASEAN, the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation affirmed support for applying international law and norms of responsible behavior in cyberspace (ASEAN, 2018). The opening for signature in Hanoi in October 2025 of the United Nations Convention against Cybercrime, adopted by the General Assembly in Resolution 79/243 of 24 December 2024, illustrates Vietnam's increasingly prominent role in international cooperation in this field (UN General Assembly, 2024).

According to the public sources available to the author, Vietnam has not issued a complete, formal, stand-alone instrument setting out its national position on how specific rules of international law apply to cyber operations, as several European and American states and the African Union have done. This is a notable policy gap: with

© 2026 by the authors; licensee Scientific Hub

international disagreement persisting over the scope of the sovereignty rule, publishing its own position would both contribute to the formation of state practice and help Vietnam locate itself in the debate.

5.14. Challenges And Recommendations

5.14.1. Principal Challenges

First, the uncertainty of the international rule. There is no consensus on the content, violation threshold, and manner of invoking the sovereignty rule, making legal responses to cyber operations below the threshold of force uncertain. *Second*, difficulties of attribution and proof. Even where the rule is recognized, attributing conduct to a state requires high technical and legal capacity, and the risk of politicized attribution is considerable. *Third*, jurisdictional conflict and the risk of fragmentation. Many states simultaneously extending their jurisdiction and imposing data-localization and content controls may produce overlapping obligations for transnational enterprises and fragment the Internet (Kohl, 2017). *Fourth*, the need to balance sovereignty, digital economic development, and human rights. Measures protecting sovereignty must satisfy legality, necessity, and proportionality under international human rights standards (International Covenant on Civil and Political Rights, 1966). This matters particularly because Politburo Resolution No. 57-NQ/TW sets a goal of breakthroughs in science, technology, innovation, and national digital transformation, which requires a legal environment favorable to investment and data flows.

6. Recommendations

1. *Publish a national position on the application of international law in cyberspace.* Vietnam should consider issuing an official document, or submitting national contributions to United Nations forums, setting out its views on the application of sovereignty as a principle with legal consequences, the violation threshold, the duty of due diligence, and the conditions for attribution and countermeasures. This is consistent with the trend among many states and regions and would increase the predictability of foreign policy.
2. *Complete the implementing instruments of the 2025 Law on Cybersecurity in a transparent and proportionate manner.* Implementing decrees should specify the criteria for determining important information systems, the scope and conditions of data-storage obligations, the procedures for requesting removal of information, and mechanisms for complaint and oversight. Such detail would both ensure effective enforcement and meet the requirements of legality and proportionality in human rights law.
3. *Design data-sovereignty measures in light of international commitments.* Vietnam should periodically review the impact of data-localization requirements on international trade commitments and on the needs of the digital economy, and adopt a risk-based approach (data classification, conditional transfer mechanisms) rather than blanket application.
4. *Strengthen capacity to meet the duty of due diligence.* This means consolidating the national incident-response system, mechanisms for sharing threat information with ASEAN and international partners, and procedures for receiving and handling assistance requests from other states. This both protects Vietnam's sovereignty and prevents domestic infrastructure from being exploited for cross-border attacks.
5. *Improve attribution capacity and prevent abuse.* Vietnam should develop procedures for independent evaluation of technical evidence, coordinated among technical, diplomatic, and legal agencies, before reaching attribution conclusions or invoking countermeasures, in order to ensure the standard of proof and avoid unnecessary escalation.
6. *Strengthen judicial cooperation and treaty engagement.* Vietnam should consider acceding to and implementing international cybercrime treaties, including the United Nations Convention, and promote bilateral mutual legal assistance arrangements to resolve jurisdictional conflicts over data.
7. *Invest in human resources specialized in international law in cyberspace.* This means training legal, diplomatic, and technical officials with interdisciplinary knowledge, participating regularly in United Nations and ASEAN forums, and expanding domestic academic research.

7. Conclusion

This article has shown that national sovereignty in cyberspace is a legal concept with real substance, even though the debate over its scope and nature has not closed. Theoretically, the layered model explains why cyberspace does not escape sovereignty: infrastructure, persons, and activities are always tied to the territory of a state. Legally, state consensus in the GGE and OEWG processes that existing international law applies, together with increasingly rich practice, supports the conclusion that sovereignty underpins jurisdiction, the principle of non-intervention, the duty of due diligence, and the regime of state responsibility. The author maintains that treating sovereignty as a rule with a carefully defined violation threshold is consistent with legal history and meets the need to fill the "gray zone" between lawful conduct and the use of force.

For Vietnam, the 2025 Law on Cybersecurity consolidates the domestic framework and supplies important instruments for protecting sovereignty. To realize its full effect, Vietnam needs to supplement it on two sides. The external side is a clear national position on the application of international law. The internal side is transparent, proportionate enforcement mechanisms that respect human rights. Ultimately, sovereignty in cyberspace is not only a right of control but also a responsibility of the state to ensure a safe, stable cyberspace that serves development. That is also the direction best suited to the long-term interests of a country accelerating its digital transformation.

8. Limitations and Future Research

This study relies on publicly available state positions and on doctrinal analysis. It does not include interviews or confidential government material. Positions of states continue to evolve, and the permanent mechanism established after the 2021–2025 OEWG may generate new practice. The Law on Cybersecurity of 2025 had not yet entered into force when the source analysis was prepared, and its implementing decrees were not available for

© 2026 by the authors; licensee Scientific Hub

analysis. Future research could examine implementation data after 1 July 2026, compare Southeast Asian states' positions, and assess the compatibility of data-localization measures with specific trade commitments.

References

African Union Peace and Security Council. (2024). Common African position on the application of international law to the use of information and communication technologies in cyberspace. African Union.

ASEAN. (2018, April 27). ASEAN leaders' statement on cybersecurity cooperation. ASEAN Secretariat. https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/

ASEAN Main Portal+1

Barlow, J. P. (1996, February 8). A declaration of the independence of cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Buchan, R. (2018). Cyber espionage and international law. Hart Publishing.

Charter of the United Nations, June 26, 1945, 1 U.N.T.S. XVI.

China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan, & Uzbekistan. (2015). Letter dated January 9, 2015, to the Secretary-General: International code of conduct for information security (U.N. Doc. A/69/723).

Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V (2018).

Constitution of the Socialist Republic of Viet Nam (2013, as amended by Resolution No. 203/2025/QH15).

Convention on Cybercrime, November 23, 2001, ETS No. 185.

Convention on Rights and Duties of States, December 26, 1933, 165 L.N.T.S. 19.

Corfu Channel Case (United Kingdom v. Albania), Merits, 1949 I.C.J. 4 (April 9).

Corn, G. P., & Taylor, R. (2017). Sovereignty in the age of cyber. AJIL Unbound, 111, 207–212.

Delerue, F. (2020). Cyber operations and international law. Cambridge University Press.

Federal Government of Germany. (2021). On the application of international law in cyberspace: Position paper. Federal Foreign Office. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. American Journal of International Law, 110(3), 425–479.

Goldsmith, J., & Wu, T. (2006). Who controls the Internet? Illusions of a borderless world. Oxford University Press.

Government of the Netherlands. (2019). Letter to the Parliament on the international legal order in cyberspace: Appendix: International law in cyberspace.

Government of Viet Nam. (2022). Decree No. 53/2022/ND-CP of August 15, 2022, detailing a number of articles of the Law on Cybersecurity.

International Covenant on Civil and Political Rights, December 16, 1966, 999 U.N.T.S. 171.

International Law Commission. (2001). Draft articles on responsibility of States for internationally wrongful acts. Yearbook of the International Law Commission, 2001, II(Part Two). https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Island of Palmas Case (Netherlands v. United States), 2 R.I.A.A. 829 (1928).

Jensen, E. T., & Watts, S. (2017). A cyber duty of due diligence: Gentle civilizer or crude destabilizer? Texas Law Review, 95(7), 1555–1577.

Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. Stanford Law Review, 48(5), 1367–1402.

Koh, H. H. (2012). International law in cyberspace. Harvard International Law Journal Online, 54, 1–12.

Kohl, U. (Ed.). (2017). The net and the nation state: Multidisciplinary perspectives on Internet governance. Cambridge University Press.

Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), Merits, Judgment, 1986 I.C.J. 14 (June 27).

Ministry of Foreign Affairs of the People's Republic of China, & Cyberspace Administration of China. (2017). International strategy of cooperation on cyberspace.

National Assembly of Viet Nam. (2015). Penal Code No. 100/2015/QH13 (as amended by Law No. 12/2017/QH14).

National Assembly of Viet Nam. (2018). Law on Cybersecurity No. 24/2018/QH14.

National Assembly of Viet Nam. (2024). Law on Digital Data No. 60/2024/QH15.

National Assembly of Viet Nam. (2025a). Law on Cybersecurity No. 116/2025/QH15. https://vanban.chinhphu.vn/?classid=&docid=216499&pageid=27160

National Assembly of Viet Nam. (2025b). Law on Personal Data Protection No. 91/2025/QH15. https://bocongan.gov.vn/chinh-sach-phap-luat/co-so-du-lieu-van-ban/luat-bao-ve-du-lieu-ca-nhan-1753688803

Ney, P. C., Jr. (2020, March 2). DOD general counsel remarks at U.S. Cyber Command legal conference. U.S. Department of Defense.

Politburo of the Communist Party of Viet Nam. (2018a). Resolution No. 29-NQ/TW of July 25, 2018, on the strategy for defending the Fatherland in cyberspace.

Politburo of the Communist Party of Viet Nam. (2018b). Resolution No. 30-NQ/TW of July 25, 2018, on the national cybersecurity strategy.

Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 2010 I.C.J. 14 (April 20).

République française, Ministère des Armées. (2019). Droit international appliqué aux opérations dans le cyberespace.

Roscini, M. (2014). Cyber operations and the use of force in international law. Oxford University Press.

Russian Federation. (2019). Federal Law No. 90-FZ of May 1, 2019, on amending the Federal Law on Communications and the Federal Law on Information, Information Technologies and Information Protection.

S.S. Lotus (France v. Turkey), 1927 P.C.I.J. (ser. A) No. 10 (September 7).

Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2017). Respect for sovereignty in cyberspace. Texas Law Review, 95(7), 1639–1671.

Trail Smelter Case (United States v. Canada), 3 R.I.A.A. 1905 (1941).

Tsagourias, N. (2015). The legal status of cyberspace: Sovereignty redux? In N. Tsagourias & R. Buchan (Eds.), Research handbook on international law and cyberspace (pp. 13–29). Edward Elgar.

United Nations General Assembly. (2013). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (U.N. Doc. A/68/98).

United Nations General Assembly. (2015). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (U.N. Doc. A/70/174).

United Nations General Assembly. (2021a). Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (U.N. Doc. A/76/135).

United Nations General Assembly. (2021b). Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final substantive report (U.N. Doc. A/75/816).

United Nations General Assembly. (2024). United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes (U.N. Doc. A/RES/79/243). https://digitallibrary.un.org/record/4071955

United Nations Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025). Final report (U.N. Doc. A/80/257). United Nations. https://digitallibrary.un.org/record/4087789

Digital Library+1

Wright, J. (2018, May 23). Cyber and international law in the 21st century [Speech]. Chatham House, London. UK Government.

Xi, J. (2015, December 16). Remarks at the opening ceremony of the Second World Internet Conference. Wuzhen, China.

© 2026 by the authors; licensee Scientific Hub