

CYBERSECURITY, SOVEREIGNTY, AND INTERNATIONAL LAW: NORMATIVE CHALLENGES IN THE DIGITAL AGE

CIBERSEGURANÇA, SOBERANIA E DIREITO INTERNACIONAL: DESAFIOS NORMATIVOS NA ERA DIGITAL

Article received on: 11/3/2025

Article accepted on: 2/2/2026

Hakan Cora*

*Onbes Kasim Kibris University, Nicosia, Cyprus

Orcid: <https://orcid.org/0000-0001-5780-549X>

corahakan@gmail.com

Elnur Hasan Mikail**

**Kafkas University, Kars, Turkey

Orcid: <https://orcid.org/0000-0001-9574-4704>

emikail@turansam.org

The authors declare that there is no conflict of interest

Abstract

Cyber operations now occupy a central position in strategic competition, yet international law continues to face persistent normative uncertainty regarding sovereignty, prohibited intervention, use of force, attribution, and permissible countermeasures. This article examines the sovereignty debate in cyberspace and argues that the primary challenge is not the absence of applicable law but the lack of shared interpretive consensus and operational thresholds. Drawing on the UN process on responsible state behaviour, the law of state responsibility, and the Tallinn Manual's restatement approach, the study maps the principal legal tests invoked by states—sovereignty, due diligence, non-intervention, use of force or armed attack, and countermeasures—and analyzes how core technical characteristics of cyberspace complicate their application. Methodologically, the article combines doctrinal legal analysis with structured qualitative illustration drawn from widely discussed incident types, including industrial disruption malware and supply-chain compromise. The findings identify three recurring normative gaps: disagreement over the legal status of sovereignty, inconsistent thresholds for coercion and effects, and underdeveloped evidentiary standards for attribution. The article concludes by proposing incremental pathways for legal stabilization aimed at enhancing predictability and restraint in the cyber domain.

Keywords: Cybersecurity. Sovereignty. International Law. State Responsibility. Cyber Operations.

Resumo

As operações cibernéticas ocupam agora uma posição central na competição estratégica, mas o direito internacional continua a enfrentar uma incerteza normativa persistente em relação à soberania, intervenção proibida, uso da força, atribuição e contramedidas permitidas. Este artigo examina o debate sobre soberania no ciberespaço e argumenta que o principal desafio não é a ausência de legislação aplicável, mas a falta de consenso interpretativo comum e de limites operacionais. Com base no processo da ONU sobre comportamento responsável dos Estados, na lei da responsabilidade dos Estados e na abordagem de reafirmação do Manual de Tallinn, o estudo mapeia os principais testes jurídicos invocados pelos Estados — soberania, diligência devida, não intervenção, uso da força ou ataque armado e contramedidas — e analisa como as características técnicas essenciais do ciberespaço complicam sua aplicação. Metodologicamente, o artigo combina análise jurídica doutrinária com ilustração qualitativa estruturada extraída de tipos de incidentes amplamente discutidos, incluindo malware de interrupção industrial e comprometimento da cadeia de suprimentos. As conclusões identificam três lacunas normativas recorrentes: desacordo sobre o status jurídico da soberania, limites inconsistentes para coerção e efeitos e padrões de evidência subdesenvolvidos para atribuição. O artigo conclui propondo caminhos incrementais para a estabilização jurídica com o objetivo de aumentar a previsibilidade e a restrição no domínio cibernético.



Palavras-chave: Segurança Cibernética.
Soberania. Direito Internacional.
Responsabilidade do Estado. Operações
Cibernéticas.

1 INTRODUCTION

Cyber operations have moved from the periphery of international security into the core of contemporary statecraft, functioning not only as tools of espionage but also as instruments of influence, disruption, and strategic signaling across peacetime and crisis settings. Unlike traditional military actions, cyber operations operate within a domain characterized by technical opacity, jurisdictional fragmentation, and pervasive civilian–military entanglement, which together complicate the application of established legal categories. As states increasingly rely on cyber capabilities to pursue national interests while avoiding overt escalation, international law faces mounting pressure to clarify how foundational principles—particularly sovereignty, non-intervention, and responsibility—apply in this digitally mediated environment (Nye, 2010). The resulting legal ambiguity is not merely a theoretical concern: uncertainty over the legality of cyber conduct reshapes strategic incentives, encourages risk-taking below traditional thresholds of force, and undermines the stabilizing function of law in managing interstate competition (Kello, 2017).

A foundational challenge is that cyberspace blurs the line between military and civilian objects, often routing operations through private infrastructure and third states, which complicates attribution and responsibility even when harm is significant (International Law Commission, 2001). At the same time, due diligence expectations—often traced to the idea that a state should not knowingly allow its territory to be used for acts contrary to the rights of other states—have renewed relevance in cyber contexts, especially for botnets, safe havens, and compromised infrastructure (International Court of Justice, 1949).

This article therefore asks: What are the core normative challenges for sovereignty-based legal ordering in cyberspace, and which doctrinal pathways most

plausibly reduce uncertainty without rewriting the entire system? (Tsagourias & Buchan, 2015).

The argument advanced is twofold: first, the legal toolkit already contains workable components (sovereignty, due diligence, state responsibility, countermeasures), but second, the absence of shared thresholds—particularly for “intrusion,” “coercion,” and “effects” —creates space for opportunistic interpretation and strategic ambiguity (Hathaway *et al.*, 2012).

To make this claim concrete, the article synthesizes leading legal scholarship and UN normative processes, then applies them through structured illustration of widely discussed incident types—industrial disruption malware and supply-chain compromise—to show how legal characterization diverges in practice (Willett, 2021).

Beyond doctrinal uncertainty, the struggle over cyber sovereignty must also be understood as part of a broader transformation in how power, interdependence, and legal authority interact in the international system. Cyberspace is not merely a new operational domain but a structural environment in which states exercise influence through control over digital infrastructure, standards, platforms, and data flows, often below the threshold of armed conflict. This condition intensifies legal ambiguity because it blurs the distinction between lawful competition and unlawful coercion, encouraging states to exploit gray zones where economic, technological, and security instruments converge. As a result, sovereignty claims in cyberspace increasingly reflect not only territorial integrity but also the capacity to shape network dependencies and vulnerabilities across borders, challenging traditional assumptions about consent, jurisdiction, and responsibility in international law (Farrell & Newman, 2019).

2 LITERATURE REVIEW

The literature on international law and cyber operations has grown into a distinct interdisciplinary field spanning public international law, security studies, and technology governance, with major syntheses emphasizing both continuity with existing doctrine and the special problems posed by cyber technicalities (Tsagourias & Buchan, 2015). A central reference point is the Tallinn Manual 2.0, which consolidates expert views on how international law applies across peacetime and conflict settings while explicitly

revealing areas of disagreement, especially sovereignty and countermeasures (Schmitt, 2017).

On sovereignty, scholarship diverges between those who treat sovereignty as an independent rule whose violation can occur through certain intrusions and those who treat it primarily as a principle that informs other rules (e.g., non-intervention), with important implications for what counts as an internationally wrongful act (Jensen, 2014). This debate also intersects with due diligence: if sovereignty violations are difficult to define, states may instead foreground duties of care to prevent harmful cyber activity emanating from their territory or infrastructure (International Court of Justice, 1949).

A parallel strand focuses on *jus ad bellum* thresholds—use of force and armed attack—and highlights that cyber operations can generate severe consequences while remaining legally contested because “effects” are hard to quantify and causal chains can be unclear (International Court of Justice, 1986).

Related work on state responsibility emphasizes that attribution and evidentiary standards are often the practical bottleneck, because legal consequences depend on linking conduct to a state under attribution rules rather than merely identifying a technical actor (International Law Commission, 2001).

Institutionally, the UN cyber norms processes—especially the Groups of Governmental Experts (GGEs) and the broader UN discussions on responsible state behaviour—serve as a key reference for emerging expectations about restraint, cooperation, and the application of international law (United Nations, 2021).

Finally, the governance literature stresses that cybersecurity is not only about armed conflict: surveillance, platform control, and the political economy of digital infrastructure shape how states understand “sovereignty” in practice, expanding the concept beyond territoriality toward informational and infrastructural control (Deibert, 2013).

3 METHODOLOGY

This study uses a **doctrinal legal method** to interpret core rules implicated by cyber operations—sovereignty, non-intervention, due diligence, use of force/armed attack, and countermeasures—by reading them through authoritative sources (ICJ

jurisprudence, ILC Articles) and leading interpretive restatements (Schmitt, 2017). Doctrinal analysis is appropriate because the normative challenge is not only empirical frequency of incidents but the legal characterization of contested conduct under existing secondary rules of responsibility (International Law Commission, 2001).

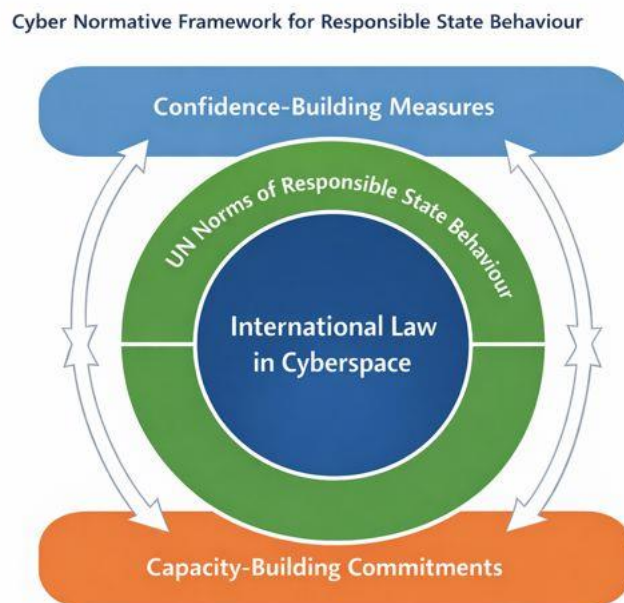
To connect doctrine with operational reality, the article applies **structured qualitative illustration** using widely documented incident-types that have shaped legal debate: (1) cyber operations designed to produce physical or industrial disruption and (2) supply-chain compromise used for large-scale espionage access (Zetter, 2014). These illustrations are not treated as adjudicated facts but as analytically useful “stress tests” for legal thresholds and attribution expectations under uncertainty (Willett, 2021).

The analysis proceeds in three steps: (i) specify the legal tests and points of contestation; (ii) map how states and scholars frame the same conduct differently; and (iii) identify convergence options—threshold clarifications, due diligence operationalization, and confidence-building measures—consistent with UN processes on responsible behaviour (United Nations Office for Disarmament Affairs, 2025).

To enhance analytical rigor and reduce interpretive bias, the doctrinal analysis is complemented by a structured interpretive framework that treats cyber incidents as legally indeterminate scenarios rather than as settled factual records. This approach reflects the reality that most significant cyber operations are never adjudicated and are instead interpreted through competing state narratives, partial disclosures, and political signaling. By focusing on how legal arguments are constructed under conditions of evidentiary uncertainty, the study prioritizes legal reasoning in practice over definitive factual attribution. Such an interpretive method allows for systematic comparison across cases and doctrines, revealing patterns in how states invoke sovereignty, due diligence, and countermeasures to legitimize or contest cyber conduct. Methodologically, this aligns with interpretivist approaches in international law that emphasize argumentation, justification, and contestation as central components of legal norm development, particularly in emerging or technologically complex domains (Kratochwil, 2014). Figure 1 illustrates the normative architecture governing responsible state behaviour in cyberspace, emphasizing how international law operates in conjunction with UN norms, confidence-building measures, and capacity-building commitments to stabilize expectations among states.

Figure 1

Normative framework for responsible state behaviour in cyberspace (adapted from United Nations Office for Disarmament Affairs, 2022).

**4 FINDINGS**

The findings presented below synthesize doctrinal analysis and structured qualitative illustration to identify recurring patterns in how international law is interpreted and operationalized in relation to cyber operations. Rather than treating legal rules as static or self-executing, the analysis reveals how sovereignty, due diligence, non-intervention, and state responsibility are actively constructed through state practice, scholarly debate, and institutional discourse under conditions of technical uncertainty and strategic contestation. The findings therefore reflect not only areas of normative disagreement but also zones of emerging convergence, highlighting how law functions as a dynamic ordering framework in an evolving technological environment. By organizing the results around core doctrinal fault lines, the section demonstrates how interpretive fragmentation—rather than legal absence—shapes contemporary governance of cyberspace and conditions the stabilizing capacity of international law (Koskenniemi, 2005).

Finding 1: Sovereignty remains the most contested gateway norm in cyberspace

Sovereignty continues to function as the principal conceptual gateway through which cyber operations are legally assessed, yet it remains the most deeply contested norm in the cyber context. The central cleavage concerns whether sovereignty constitutes an independent rule of international law capable of direct violation through certain cyber intrusions—such as the remote implantation of malware or manipulation of digital systems—or whether it operates primarily as a foundational principle that informs the application of other rules, including non-intervention and the prohibition of the use of force (Schmitt, 2017). This divergence is not merely semantic; it has concrete legal consequences for determining when an internationally wrongful act has occurred and what responses are available to an injured state.

Where sovereignty is treated as an autonomous rule, relatively low thresholds of intrusion or functional interference may suffice to trigger legal responsibility, potentially expanding the scope for lawful countermeasures. By contrast, where sovereignty is conceptualized as a guiding principle rather than a freestanding obligation, the same conduct may be viewed as legally neutral unless it crosses established thresholds of coercion, force, or intervention (Jensen, 2014). The absence of consensus on this foundational question contributes to fragmentation in state practice and enables strategic ambiguity, as states selectively adopt interpretations that align with their operational interests.

Finding 2: Due diligence is widely endorsed but remains normatively under-specified

Due diligence has emerged as one of the most frequently invoked doctrines in discussions of state responsibility for cyber operations, reflecting its perceived compatibility with the transboundary and networked nature of cyberspace. Rooted in the obligation not to knowingly allow one's territory to be used for acts contrary to the rights of other states, due diligence appears particularly well-suited to cyber scenarios involving botnets, proxy actors, and compromised infrastructure operating across multiple jurisdictions (International Court of Justice, 1949).

Despite this apparent consensus on relevance, significant disagreement persists regarding the content and scope of due diligence obligations in cyberspace. States diverge on what constitutes sufficient “knowledge” of malicious cyber activity, what level of

technical “capacity” is required to trigger responsibility, and what measures are considered “reasonable” in light of a state’s resources and institutional capabilities (United Nations, 2021). This lack of specification weakens the doctrine’s constraining effect and risks transforming due diligence into a rhetorical device rather than an operational legal standard, particularly in relation to privately owned infrastructure and transnational service providers.

Finding 3: Non-intervention is constrained by the operational ambiguity of coercion

The prohibition on intervention in the internal or external affairs of states remains a cornerstone of international law, yet its application in cyberspace is significantly constrained by the difficulty of operationalizing the concept of coercion. Traditionally, non-intervention requires coercive interference in a state’s *domaine réservé*, compelling it to act in a manner it would not otherwise choose (International Court of Justice, 1986). In cyber contexts, however, many impactful operations influence political, economic, or social outcomes without employing overt or direct coercive pressure.

Cyber activities such as data theft, strategic leaks, and information manipulation often blur the line between persuasion, influence, and coercion, making legal characterization highly contested. As a result, states frequently acknowledge the hostile or destabilizing nature of such operations while stopping short of framing them as unlawful interventions. This pattern encourages reliance on political countermeasures, sanctions, and narrative responses rather than legal claims grounded in non-intervention, thereby marginalizing the doctrine’s practical relevance in cyber disputes (Nye, 2010).

Finding 4: Jus ad bellum thresholds remain effects-based but are difficult to operationalize

The application of jus ad bellum rules—particularly the prohibition of the use of force and the right of self-defense against armed attack—continues to rely on effects-based analysis, emphasizing scale, gravity, and consequences (Cora, 2024). In theory, this framework allows cyber operations to qualify as uses of force or armed attacks where their effects are comparable to kinetic harm (Schmitt, 2017). In practice, however, cyber effects are often indirect, cumulative, delayed, or distributed across multiple systems, complicating assessments of severity and causation.

Disruptive malware targeting industrial systems illustrates this challenge. Even where cyber operations produce physical damage or endanger human safety, uncertainty surrounding attribution, intent, and proportionality frequently prevents consensus legal characterization as a use of force or armed attack (Zetter, 2014). This ambiguity creates a persistent gray zone in which severe cyber operations remain legally contested, undermining the deterrent and signaling functions traditionally associated with *jus ad bellum* thresholds.

Finding 5: Attribution and evidentiary standards are the primary bottlenecks of responsibility

Across all doctrinal areas examined, attribution emerges as the most significant practical obstacle to the effective application of international law to cyber operations. Even where conduct appears to breach a primary rule, legal responsibility depends on attributing that conduct to a state under the secondary rules of state responsibility, including actions by state organs, entities exercising governmental authority, or non-state actors acting under direction or control (International Law Commission, 2001).

The technical complexity of cyber attribution rarely aligns neatly with these legal categories. States often possess intelligence-based assessments that they are unwilling or unable to disclose fully, leading to partial, selective, or opaque evidentiary presentations. While such practices may be strategically rational, they limit the ability of third states and international audiences to assess legal claims objectively, thereby reinforcing skepticism and contestation around responsibility assertions (United Nations, 2021).

Finding 6: Countermeasures dominate state practice but remain legally fragile

In the absence of clear *jus ad bellum* thresholds, countermeasures have become a central response mechanism for states confronting allegedly unlawful cyber operations. Countermeasures offer a legally grounded alternative to force, allowing injured states to induce compliance through proportionate and reversible measures (International Law Commission, 2001). However, applying traditional countermeasure requirements in cyberspace presents significant challenges.

Cyber operations unfold at a speed and scale that strain legal expectations of prior notification, opportunity for compliance, and proportionality assessment. Moreover, the difficulty of reversibility in digital systems—where effects may cascade unpredictably—raises questions about whether cyber countermeasures can reliably meet established legal

constraints. This tension between operational necessity and legal discipline widens the gap between normative expectations and actual state behavior, incentivizing secrecy and unilateralism (Hathaway *et al.*, 2012).

Finding 7: Supply-chain compromise intensifies sovereignty and shared responsibility dilemmas

Large-scale supply-chain intrusions represent a particularly acute stress test for sovereignty and responsibility frameworks. Such operations are often framed as espionage and thus treated as falling below the threshold of illegality, yet their systemic consequences—widespread access, latent vulnerability creation, and long-term security degradation—challenge this characterization (Willett, 2021). The distinction between lawful intelligence gathering and unlawful intrusion becomes increasingly unstable when access itself undermines the integrity of critical systems.

Because supply-chain operations implicate multiple jurisdictions, private actors, and layers of dependency, they also magnify questions of shared responsibility and cooperative obligations. These dynamics highlight the growing importance of infrastructural dependence in sovereignty claims, suggesting a shift from territorially bounded notions of control toward more network-oriented understandings of legal authority and vulnerability (Deibert, 2013).

4.1 Overall synthesis of findings

Taken together, the findings demonstrate that the principal normative challenge in cyberspace is not the absence of applicable legal rules but the fragmentation of interpretive consensus across core doctrines. Sovereignty, due diligence, non-intervention, *jus ad bellum* thresholds, attribution, and countermeasures each provide partial regulatory guidance, yet none operates with sufficient clarity or institutional support to stabilize expectations consistently. This fragmentation enables strategic exploitation of legal ambiguity and weakens the coordinating function of international law in managing cyber competition (United Nations, 2021). Table 1 synthesizes the article's core findings by mapping foundational doctrines of international law onto the specific normative challenges posed by cyber operations, highlighting where traditional legal functions encounter interpretive strain. By juxtaposing doctrinal purpose with

cyber-specific disruption, the table illustrates how fragmentation across legal thresholds collectively undermines the stabilizing role of international law in the digital domain.

Table 1

Core International Law Doctrines and Their Normative Challenges in Cyberspace

Legal Doctrine	Classical Legal Function	Primary Challenge in Cyberspace	Implications for Legal Stability
Sovereignty	Establishes territorial authority and independence of states	Lack of consensus on whether sovereignty is an independent rule or a guiding principle; uncertainty over what constitutes a relevant cyber intrusion	Fragmented thresholds for wrongfulness; expanded space for strategic ambiguity and inconsistent countermeasures
Due Diligence	Obligates states not to knowingly allow harm to other states from their territory	Ambiguity regarding knowledge, capacity, and reasonable measures in relation to private and transnational cyber infrastructure	Weak operationalization risks reducing due diligence to a rhetorical norm rather than an enforceable obligation
Non-Intervention	Prohibits coercive interference in a state's domaine réservé	Difficulty operationalizing coercion in indirect, influence-based cyber operations	Marginalization of non-intervention in practice; increased reliance on political rather than legal responses
Use of Force / Armed Attack	Regulates escalation and self-defense under jus ad bellum	Challenges in measuring cyber "effects," causation, and intent; delayed and distributed harm	Persistent gray zone below armed conflict thresholds; weakened deterrence and escalation control
Attribution (State Responsibility)	Links wrongful conduct to a state under secondary rules	Mismatch between technical attribution and legal standards; limited evidence disclosure	Reduced credibility of legal claims; erosion of trust and normative convergence
Countermeasures	Enables proportionate, non-forcible responses to wrongful acts	Difficulty applying necessity, proportionality, and reversibility at cyber speed	Risk of unilateralism and legal erosion if constraints remain under-specified
Supply-Chain Integrity	Not traditionally regulated as a separate legal category	Systemic vulnerability across multiple jurisdictions and private actors	Pressure to reconceptualize sovereignty and responsibility in network-dependent environments

5 DISCUSSION

The findings collectively underscore that the central challenge facing international law in the cyber domain is not doctrinal insufficiency but interpretive fragmentation under conditions of strategic and technological uncertainty. Across sovereignty, due diligence, non-intervention, jus ad bellum thresholds, attribution, and countermeasures, the analysis reveals a recurring pattern: legal rules exist and are widely invoked, yet their stabilizing capacity is weakened by divergent thresholds, contested meanings, and uneven institutionalization. This fragmentation transforms international law from a coordinating framework into a site of contestation, where legal argumentation itself becomes an instrument of statecraft rather than a shared constraint on behavior (United Nations, 2021).

A key implication of the findings is that sovereignty's contested status functions as a multiplier of uncertainty across the entire legal architecture governing cyber operations. Where sovereignty is treated as an independent rule, it lowers the entry point for legal wrongfulness and expands the potential space for countermeasures; where it is treated as a background principle, legal responsibility is deferred to higher thresholds such as coercion or force. This divergence does not merely reflect academic disagreement but mirrors strategic preferences, allowing states to calibrate legal interpretations to operational objectives (Kello, 2017). As a result, sovereignty debates in cyberspace exemplify a broader phenomenon in international law: the increasing use of legal indeterminacy as a resource rather than a problem to be resolved.

The findings on due diligence further reinforce this dynamic. While due diligence enjoys broad rhetorical endorsement, its operational content remains weakly specified, particularly with respect to cyber infrastructure that is privately owned, transnationally distributed, and technically opaque. This under-specification enables states to invoke due diligence selectively—either to externalize responsibility for malicious cyber activity or to resist obligations perceived as overly burdensome. In doing so, due diligence risks evolving into a norm of expectation rather than obligation, diminishing its capacity to shape behavior consistently. Yet, the same findings also suggest that due diligence represents one of the most promising pathways for incremental normative consolidation,

precisely because it accommodates variation in capacity while preserving a shared baseline of responsibility.

The analysis of non-intervention and coercion highlights a deeper structural tension between classical legal categories and contemporary modes of influence. Cyber operations frequently operate through indirect, cumulative, and deniable mechanisms that shape outcomes without issuing explicit demands or threats. This challenges the coercion-based logic that underpins the non-intervention rule and explains why many cyber activities are widely regarded as hostile yet rarely framed as unlawful. The consequence is a growing reliance on political and economic responses—sanctions, attribution statements, and counter-influence measures—rather than legal claims grounded in non-intervention. Over time, this pattern risks marginalizing the doctrine, reducing its relevance in precisely those contexts where legal restraint would be most valuable.

The findings relating to *jus ad bellum* thresholds further illustrate how effects-based analysis, while theoretically adaptable, encounters practical limits in cyberspace. Although there is broad agreement that cyber operations may constitute a use of force or armed attack if their consequences are sufficiently grave, persistent disagreement over how to measure effects, establish causation, and assess intent undermines consensus. This ambiguity is compounded by attribution challenges, which frequently prevent states from advancing legal claims with sufficient confidence or evidentiary support. The resulting gray zone allows severe cyber operations to remain legally contested, weakening deterrence and complicating escalation management.

Attribution and evidentiary practices emerge from the findings as the critical hinge between legal theory and operational reality. Even where primary rules appear violated, the inability or unwillingness of states to disclose evidence in a transparent and standardized manner undermines the credibility of responsibility claims. This has systemic consequences: it erodes trust, enables counter-accusations, and reinforces skepticism toward legal argumentation in cyber disputes. The findings suggest that attribution should be understood not merely as a technical challenge but as a normative and institutional one, central to the functioning of international law in a domain characterized by secrecy and intelligence asymmetries.

The growing reliance on countermeasures, as identified in the findings, reflects both the adaptability and fragility of the existing legal framework. Countermeasures offer

a means of responding to unlawful cyber operations without resorting to force, aligning with the preference for escalation control in cyberspace. However, the difficulty of applying traditional constraints—necessity, proportionality, reversibility, and prior notification—at cyber speed raises concerns about legal erosion. If countermeasures become normalized without corresponding clarification of their limits, they risk reinforcing unilateralism and undermining the reciprocal discipline that the law of state responsibility is designed to promote.

Finally, the discussion of supply-chain compromise points to a structural shift in how sovereignty and responsibility are experienced in practice. Large-scale intrusions that exploit infrastructural dependencies challenge territorially grounded conceptions of control and blur the line between access and harm. These operations reveal that sovereignty claims increasingly hinge on systemic integrity rather than physical location, suggesting an evolution toward network-oriented understandings of legal authority. This shift does not render existing doctrines obsolete, but it does require reinterpretation that accounts for interdependence, shared vulnerability, and the central role of private actors in cyber ecosystems.

Taken together, the research indicates that legal stabilization in cyberspace is most likely to emerge through incremental clarification rather than comprehensive reform. Effects-based thresholds, operationalized due diligence, improved attribution transparency, and confidence-building measures within existing UN processes offer pragmatic avenues for reducing uncertainty while preserving legal flexibility. The challenge lies not in inventing new rules, but in fostering sufficient convergence around interpretive practices to allow international law to perform its coordinating and restraining functions in the digital age.

The findings suggest that the normative challenge is less a “legal vacuum” than a coordination problem: states possess overlapping legal vocabularies but disagree on thresholds and on the evidentiary posture required to make legal claims credible (United Nations, 2021).

This coordination problem is exacerbated by strategic ambiguity, because states may benefit from preserving interpretive flexibility for their own operations while demanding strict readings for adversaries (Kello, 2017).

A promising pathway is effects-based threshold clarification that does not require rewriting *jus ad bellum* but does require shared guidance on cyber-specific indicators of gravity, including functional disruption of essential services, interference with safety systems, and systemic integrity compromise (Schmitt, 2017). Such clarification would not eliminate disagreement, but it could narrow the zone where states plausibly disagree about whether an operation is merely unfriendly, unlawful, or escalatory (International Court of Justice, 1986).

Second, operationalizing due diligence for critical infrastructure would align with longstanding principles while addressing modern risk: states could converge on expectations for incident response cooperation, botnet mitigation, and protection of core public services, especially where “knowledge” and “capacity” are demonstrable (International Court of Justice, 1949). The UN processes already provide a political platform for this convergence by promoting norms, confidence-building measures, and cooperative capacity-building that can stabilize expectations without formal treaty change (United Nations Office for Disarmament Affairs, 2025).

Third, attribution transparency and evidentiary practices should be treated as a legal-stability issue, not only a technical one: limited, standardized disclosure—sources, methods, confidence levels—could make legal claims more assessable and reduce incentives for opportunistic counter-accusation (International Law Commission, 2001). Over time, such practices could strengthen the credibility of responsibility claims and make countermeasures more legally disciplined, narrowing the gap between operational cyber response and the law of state responsibility (Hathaway *et al.*, 2012).

6 CONCLUSION

This article has argued that international law possesses the conceptual and doctrinal resources necessary to regulate state behavior in cyberspace, yet sovereignty-centered legal ordering remains unstable due to persistent interpretive fragmentation rather than normative absence. Disagreement over whether sovereignty constitutes an independent rule, uncertainty surrounding thresholds of coercion and effects, and the lack of institutionalized standards for attribution collectively weaken the law’s capacity to provide predictable guidance and restraint. These challenges are not merely technical or

transitional; they reflect deeper tensions between established legal frameworks and the strategic realities of a digitally networked international system (Schmitt, 2017).

By systematically mapping how states and scholars invoke sovereignty, due diligence, non-intervention, *jus ad bellum* thresholds, and countermeasures, the article demonstrates that legal ambiguity functions as a structural feature of contemporary cyber governance. In this environment, international law operates simultaneously as a constraint and a strategic resource, shaping behavior not only through formal prohibition but also through contested interpretation. Recognizing this dual function is essential for understanding why cyber operations persist below traditional thresholds of force and why legal consensus remains elusive despite widespread affirmation that international law applies in cyberspace (United Nations, 2021).

The analysis further shows that pathways toward greater normative stability do not require wholesale revision of the international legal order. Instead, incremental clarification—particularly of effects-based thresholds, operational due diligence expectations for critical infrastructure, and evidentiary practices for attribution—offers a realistic and legally coherent route toward reducing uncertainty. Such clarification would strengthen the coordinating role of international law while preserving the flexibility necessary to accommodate technological change and diverse state capacities.

The contribution of this manuscript lies in reframing the cyber sovereignty debate as a problem of interpretive coordination rather than legal deficiency. By integrating doctrinal analysis with structured qualitative illustration, the study advances a more nuanced understanding of how international law functions under conditions of technological opacity and strategic contestation. In doing so, it contributes to both international legal scholarship and cybersecurity governance by clarifying the mechanisms through which legal norms evolve, stabilize, or fragment in emerging domains. Ultimately, the article underscores that the future effectiveness of international law in cyberspace will depend less on the creation of new rules than on the cultivation of shared interpretive practices capable of sustaining legal accountability and strategic restraint in the digital age.

REFERENCES

- Cora, A. N. (2024). Exploring the viability and implications of a NATO-like defense cooperation among Turkic states. *Türk Dünyası İncelemeleri Dergisi*, 24(2), 627–642. <https://doi.org/10.32449/egetdid.1538388>
- Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. Council of Europe.
- Deibert, R. J. (2013). *Black code: Surveillance, privacy, and the dark side of the Internet*. McClelland & Stewart.
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Organization*, 73(1), 42–79. <https://doi.org/10.1017/S0020818318000457>
- Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 100(4), 817–885.
- International Court of Justice. (1949). *Corfu Channel (United Kingdom v. Albania), Judgment of 9 April 1949*. <https://www.icj-cij.org>
- International Court of Justice. (1986). *Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of 27 June 1986*. <https://www.icj-cij.org>
- International Law Commission. (2001). *Draft articles on responsibility of states for internationally wrongful acts, with commentaries (UN Doc. A/56/10)*. United Nations.
- Jensen, E. T. (2014). Cyber sovereignty: The way ahead. *Texas International Law Journal*, 50, 275–305.
- Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- Koskenniemi, M. (2005). *From apology to utopia: The structure of international legal argument* (Reissue ed.). Cambridge University Press.
- Kratochwil, F. (2014). *The status of law in world society: Meditations on the role and rule of law*. Cambridge University Press.
- Nye, J. S., Jr. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Tsagourias, N., & Buchan, R. (Eds.). (2015). *Research handbook on international law and cyberspace*. Edward Elgar Publishing.

- United Nations Office for Disarmament Affairs. (2022). *The UN norms of responsible state behaviour in cyberspace (Figure 2: The four components that make up the UN framework of responsible state behaviour in cyberspace) [Adapted]*. United Nations. <https://documents.unoda.org>
- United Nations Office for Disarmament Affairs. (2025). *Developments in the field of information and telecommunications in the context of international security*. <https://disarmament.unoda.org>
- United Nations. (2021). *Report of the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (UN Doc. A/76/50)*. United Nations.
- Willett, M. (2021). Lessons of the SolarWinds hack. *Survival*, 63(2), 7–26. <https://doi.org/10.1080/00396338.2021.1906001>
- Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishers.

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Cora, H., & Mikail, E. H. (2026). CYBERSECURITY, SOVEREIGNTY, AND INTERNATIONAL LAW: NORMATIVE CHALLENGES IN THE DIGITAL AGE. *Veredas Do Direito*, 23, e234381. <https://doi.org/10.18623/rvd.v23.4381>