International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 09 Issue 03 March 2026

DOI: 10.47191/ijsshr/v9-i3-76, Impact factor- 8.361

Page No: 2346-2350

The Latent Impact of Cyber Attacks on the Principle of Sovereignty Under International Law

Dyah Ayu Kusumawicitra[1], Joko Setiyono[2]

[1,2]Master of Law, Diponegoro University, Semarang

ABSTRACT: The advancement of information technology has ushered in a new era of global threats, one of which is cyberattacks that are latent and not always immediately detectable. In the context of inter-state relations, cyberattacks pose a serious challenge to one of the fundamental principles of international law: the principle of sovereignty. The ambiguity of perpetrators, the obscured origin of the attacks, and the often intangible damages make it difficult to identify violations that are legally actionable. This study aims to analyze how latency in cyberattacks affects the enforcement of state sovereignty from the perspective of international law. The findings reveal that latent cyberattacks create a legal grey area in attributing state responsibility, especially when attacks are carried out by non-state actors or through the territory of third-party states. Furthermore, the principles of non-intervention and the prohibition on the use of force are challenged, as not all cyberattacks meet the threshold of "use of force" as outlined in the UN Charter. These conditions demand the development of international legal norms that are more adaptive to the nature of cyber warfare, particularly in terms of detection, attribution, and dispute resolution mechanisms. In the long run, the inability of international law to effectively address cyber threats could undermine the stability of the international system and open the door to conflict escalation. Therefore, legal reform and strengthened multilateral cooperation are urgently needed to uphold state sovereignty in the digital era.

KEYWORDS: Cyberattack; State Sovereignty; International Law; Latency; Non-Intervention

I. INTRODUCTION

In the current era of digital globalization, the international community faces increasingly complex challenges in safeguarding state sovereignty. One of the most significant challenges arises from cyberspace, where cross-border activities may be carried out instantaneously, without authorization, and often beyond direct traceability. Cyber attacks not only affect information technology systems but also extend to vital sectors such as defense, economy, health, and public infrastructure. When a State suffers systemic disruption as a result of a cyber attack, such an act essentially constitutes a violation of that State's integrity and internal control. (Akbar, 2024)

The primary concern, however, lies in the latent nature of such attacks manifesting effects only indirectly, concealing the identity of the perpetrators, and not readily recognizable as traditional forms of aggression. This ambiguity blurs the line between hostile acts and non-military disruptions. The uncertainty in attributing responsibility, coupled with the limitations of the current framework of international law, creates a dilemma in the enforcement of the principle of sovereignty, which has long served as the cornerstone of inter-State relations. Consequently, cyberspace has emerged as a new domain of contestation within international law, compelling States to reconstruct their understanding of sovereignty in a context that is highly dynamic and devoid of physical manifestation. (Rachman, 2021)

From an international legal perspective, the principle of sovereignty constitutes a peremptory norm that delineates the exclusive authority of a State over its territorial domain, natural resources, and internal affairs, free from external interference. As a foundational tenet of the United Nations Charter and a principle consistently reaffirmed in various international treaties and customary international law, sovereignty forms the cornerstone of the international legal order. Nevertheless, in circumstances where a State is subjected to a cyber operation originating beyond its territorial jurisdiction, which results in substantial impairment of its governmental functions and critical infrastructures, a profound legal question emerges: to what extent may such a cyber operation be construed as constituting a breach of the principle of sovereignty under international law?

A central question arises as to whether the victim State possesses the right to exercise self-defense, and what forms of response may be deemed lawful under international law. The latent nature of cyberattacks complicates the attribution of State responsibility, particularly when such operations are conducted by non-State actors or executed through infrastructures located within third States. In such circumstances, the principles of non-intervention and the prohibition on the use of force become increasingly difficult to apply in absolute terms, given that international law has not yet fully anticipated the digital dimension of contemporary threats.

Consequently, there is an imperative for the progressive development of legal norms and interpretative frameworks capable of addressing the challenges posed by the latency and invisibility of cyber operations, thereby ensuring that the principle of sovereignty does not remain a static concept but continues to retain its relevance in confronting the complexities of the evolving digital era.

II. RESEARCH METHOD

The research approach employed in this study is the Normative/Dogmatic Concept. This method emphasizes the conception of law as a system of legal rules and regulations arranged systematically in a hierarchical pyramid, the apex of which is the *grundnorm* (basic norm) serving as the ultimate source and foundation of validity for the entire body of legislation. (Marzuki, 2005) The research in this writing is qualitative in nature, in which the data are not presented in numerical form but rather in verbal expressions. Suteki, quoting Syaodih Sukmadinata, defines qualitative research as a type of research aimed at describing and analyzing phenomena, events, social activities, attitudes, beliefs, perceptions, and the thoughts of individuals as well as groups. (Noor, 2011)

The legal materials were collected through documentary research and literature study. The data analysis was conducted qualitatively by employing deductive reasoning. The collected legal materials, obtained through the process of legal inventory, were subsequently classified and subjected to an in-depth analysis by examining the underlying principles, values, and fundamental norms contained therein. This analysis was then cross-checked with other statutory regulations in order to identify the level of synchronization as well as any inconsistencies among the relevant laws and regulations. (Satjipto Rahardjo, 2004)

III. RESULTS AND ANALYSIS

A. The Impact of Cyberattack Latency on the Application of the Principle of State Sovereignty in International Law

Cyberattacks have emerged as one of the most complex forms of non-traditional threats in the current era of digital globalization, and the latent characteristics of such attacks have posed significant challenges to the application of the principle of State sovereignty under international law. Latency, in the context of cyber operations, refers to the delay in detecting, identifying, and attributing an attack in a timely and accurate manner. A State may be subjected to cyber intrusions in the form of system infiltration, data exfiltration, sabotage of critical infrastructure, or the manipulation of public opinion through disinformation, without realizing that its systems have been compromised until months or even years after the initial breach. The consequences of such latency render it difficult for the victim State to assert that its sovereignty has been violated, as international law anchored in the foundational principles of the United Nations Charter and other legal instruments requires concrete evidence of intervention by a foreign State or actor that causes harm. In the absence of clarity regarding the timing, perpetrators, and locus of the attack, the legal and diplomatic measures that the victim State might otherwise pursue are delayed or rendered altogether ineffective. This situation exposes a profound gap in the international legal system, which remains largely oriented toward physical, territorial, and immediate conceptions of violations of State sovereignty. (Yanuar, 2021)

Sovereignty encompasses the exclusive authority of a State over its territory, its population, and its internal affairs whether political, legal, economic, or socio-cultural free from external interference. However, the development of information and communication technologies has expanded the dimensions of State existence from being solely physical to also digital in nature. States today not only possess territorial domains of land, sea, and air, but also a form of "cyber territory," consisting of information networks, data, and servers administered or located within their jurisdiction. When a cyberattack occurs such as the exfiltration of data from critical ministries, the digital disruption of a national power grid, or the manipulation of content within domestic communication networks it effectively strikes at the core of a State's digital sovereignty. Yet, due to the latent nature of cyberattacks, which renders the identification of perpetrators both delayed and uncertain, the victim State lacks the immediate capacity to enforce its sovereign rights. This incapacity undermines the effectiveness of the principle of State sovereignty in international law, owing to the absence of adaptive legal instruments capable of addressing violations that occur in concealed, anonymous, and transboundary forms. (Prasetyo, 2023)

The latency of cyberattacks also exerts a profound impact on the application of the principle of non-intervention, which constitutes one of the fundamental pillars of international law. This principle explicitly prohibits any State from interfering in the internal affairs of another, whether directly or indirectly, including through digital means. However, when a State falls victim to disinformation campaigns disseminated via social media networks by foreign actors, or when its electoral system is disrupted through external cyber intrusions, such acts evidently amount to violations of the principle of non-intervention. Regrettably, in latent situations where digital evidence is difficult to verify, the victim State is unable to promptly assert such acts as unlawful intervention under international law. In the absence of robust and internationally acceptable proof, claims of violation lack legitimacy and may be easily refuted by the accused party. In such circumstances, malevolent States may exploit legal loopholes created by the latent nature of cyberattacks to pursue political, ideological, or economic agendas without fear of international sanctions. Ultimately, this dynamic erodes the credibility of international law as a safeguard of sovereign equality and opens a grey area in the implementation of global norms that are intended to uphold justice and international order. (Radsan, 2007)

Furthermore, the latency of cyberattacks directly affects a State's ability to exercise its inherent right of self-defense as enshrined in Article 51 of the United Nations Charter. International law recognizes the right of every State to defend itself in the event of an

armed attack by an external actor. However, in the cyber context, establishing that a particular operation constitutes an "armed attack" proves exceedingly difficult, especially when the attack is neither immediately visible, nor lethal, nor produces tangible effects in an observable timeframe. For instance, where a State's defense systems are gradually incapacitated by a cyber operation that infiltrates military software over the course of several months, yet the perpetrator remains unidentified and the precise timing of the attack cannot be determined, the victim State faces a profound legal dilemma: may it lawfully resort to counterforce without certainty as to the responsible party? Can it invoke military measures on the basis of unverifiable assumptions? The uncertainty generated by latency renders the principle of self-defense ineffective in the cyber domain, thereby leaving State sovereignty increasingly vulnerable to digital threats in the absence of lawful and proportionate mechanisms of response consistent with prevailing norms of international law. (Maskun, 2020)

The impact of latency in cyberattacks further exacerbates the fragmentation of international law in governing cyberspace, as States continue to develop divergent doctrines, policies, and interpretations of what constitutes a violation of sovereignty in the digital context. Some States explicitly assert that cyber operations targeting public infrastructure or national defense systems amount to sovereignty breaches warranting lawful countermeasures, whereas others contend that such cyber activities do not meet the threshold of "use of force" under the United Nations Charter This divergence of perception is compounded by the fact that many States prefer to respond covertly through retaliatory cyber operations that themselves remain undetected. Under such conditions, cyberspace has effectively become a domain of "silent warfare," populated by both State and non-State actors engaging in infiltration, data theft, and hostile operations without formal acknowledgment or oversight under international law. As a result, the principle of sovereignty has become fragmented and deprived of uniform global protection, with States increasingly relying on unilateral policies that risk escalating inter-State conflict in the digital realm. (Putra, 2018)

The latent effects of cyberattacks necessitate a serious reform of the international legal framework in order to effectively respond to the novel dynamics introduced by digital technologies. Classical principles such as sovereignty, non-intervention, and self-defense must be reconceptualized and expanded to encompass acts occurring within cyberspace. An international consensus is required to establish global standards on how cyberattacks are to be identified, how attribution to perpetrators should be determined, how their impact on sovereignty ought to be measured, and how States may lawfully and proportionately respond. Absent a comprehensive and adaptive regulatory regime, States will remain trapped in a condition of legal uncertainty, thereby creating opportunities for malicious actors to operate with impunity. In the long term, should the international community fail to adopt a robust and binding international legal instrument governing cyberspace, the principle of State sovereignty risks losing its substantive force, as it will no longer be capable of safeguarding the integrity of the State within the digital dimension now emerging as a principal arena of global power contestation.

B. Contemporary International Law's Capacity to Regulate the Latency of Cyberattacks as a Violation of State Sovereignty

Contemporary international law continues to face significant challenges in addressing the latency of cyberattacks as a form of violation of State sovereignty, primarily due to the absence of a specific and detailed legal framework governing the issues arising from the dynamics of cyberspace. While foundational principles such as State sovereignty, non-intervention, and the prohibition on the use of force have long been established as binding norms under the United Nations Charter and customary international law, the application of these principles in the cyber domain remains severely limited owing to the unique characteristics of cyber operations, particularly their latent nature. High-latency cyberattacks, which neither produce immediate effects nor reveal their presence in the short term, create serious difficulties in determining breaches of international law. Such operations may gradually infiltrate another State's digital systems, extract sensitive data, monitor activities, or implant malware that remains dormant for months before activation during which time the victim State may remain unaware that its sovereignty has already been compromised. The absence of a clear international legal mechanism regulating how States should respond to cyber operations that are detected only belatedly demonstrates that international law, in its current form, has yet to fully accommodate latent cyber intrusions as tangible violations of sovereignty. (Mustameer, 2022)

The principle of sovereignty, long regarded as a fundamental norm in inter-State relations, has not yet been adequately adapted to respond to the rapid advancement of technology, particularly in the realm of cybersecurity. While States generally concur that sovereignty encompasses control over physical territory, populations, and legal jurisdiction, there is as yet no global consensus affirming that cyberspace and its components such as digital infrastructure, communication networks, and data constitute part of sovereign territory protected under international law. As a result, when high-latency cyberattacks target vital aspects of a State's systems, such as financial structures, military communications, or energy infrastructure, the victim State cannot readily assert that a violation of sovereignty has occurred unless it can establish the direct and intentional involvement of a foreign State. This evidentiary process is exceedingly difficult, given that digital traces can be manipulated, routed through intermediaries, or executed by non-State actors. Consequently, contemporary international law remains insufficiently robust to ensure the protection of sovereignty in the context of latent cyber operations, as its principles have not yet been reinforced by specific and implementable legal instruments.

Moreover, the absence of a binding international instrument that explicitly regulates cyber operations has created a serious legal vacuum in addressing sovereignty violations in the digital domain. Although certain international organizations such as NATO, the Tallinn Manual process, and deliberations under the auspices of the United Nations have sought to develop norms of State conduct in cyberspace, such initiatives remain non-binding soft law, with implementation heavily dependent on the political will of individual States. The Tallinn Manual, for instance, as an academic guide on the application of international humanitarian law and international law in cyberspace, acknowledges that sufficiently serious cyber operations may amount to violations of sovereignty. However, since it does not carry the status of a binding international treaty, its application remains merely referential. Thus, when a State falls victim to a latent cyberattack and seeks to invoke the Tallinn Manual as a basis for establishing responsibility, the alleged perpetrating State can easily dismiss such claims on the ground that it is not legally bound by the Manual's provisions. Accordingly, in the absence of a formal international convention that clearly defines rules and sanctions for sovereignty violations through cyber operations particularly those of a latent nature it must be concluded that contemporary international law remains incapable of effectively regulating such challenges. (Puspita, 2022)

The latency inherent in cyber operations further blurs the boundary between violations of sovereignty and acts of espionage, the latter of which has traditionally been tolerated in international practice or, at the very least, not explicitly regulated as a breach of international law. Many States discreetly conduct intelligence activities against others, including through digital means, without fear of legal consequences, as no international norm expressly prohibits espionage let alone cyber-enabled espionage, which is particularly difficult to substantiate. When malware is implanted within another State's systems for the purpose of surveillance or data exfiltration, and its presence is only discovered years later, the victim State not only faces difficulties in proving a breach but also lacks effective avenues for international legal redress. In this context, latency creates a legal grey zone in which the aggressor State may conceal itself behind the complexities of digital evidence, while the victim State is deprived of a solid legal foundation to demand accountability. This reveals that contemporary international law remains overly static in the face of the dynamic nature of cyberspace and, as such, is not yet sufficiently effective in addressing sovereignty violations committed in latent form through digital technologies.

The concept of attribution under international law, which is pivotal in establishing State responsibility for violations of sovereignty, becomes exceedingly difficult to apply in cases of latent cyber operations. Under the doctrine of State responsibility, a breach of international law must be supported by compelling evidence that the wrongful act can be directly attributed to a State. However, in the cyber domain particularly in latent cyber operations perpetrators may employ a variety of techniques to obfuscate their identity, including the use of botnets, proxy servers, anonymizing networks such as TOR, or even the exploitation of third-party digital infrastructure without the knowledge of the territorial State. Such practices render attribution virtually impossible when measured against the high evidentiary threshold required by international law. In the absence of valid attribution, no State can be held legally responsible for the attack, nor can it be pursued for violations of sovereignty. This situation places victim States of latent cyber operations in a legally vulnerable position and creates a significant loophole for digital impunity, enabling perpetrators to evade accountability. Accordingly, it must be acknowledged that the current international legal framework still lacks adequate instruments to regulate and sanction sovereignty violations arising from latent cyber operations, notwithstanding the increasing urgency posed by the escalating transnational digital threat landscape. (Putra, 2018)

On the other hand, although efforts have been made to extend the application of the principle of State sovereignty into the digital domain, there remains no strong global consensus regarding its boundaries, scope, and implementation in cyberspace. Various international fora, such as the Global Commission on the Stability of Cyberspace (GCSC) and the United Nations Group of Governmental Experts (UNGGE), have proposed norms and principles aimed at preserving cyber stability, including prohibitions against cyber operations targeting another State's critical infrastructure. Nevertheless, given their voluntary and non-binding character, such norms cannot be regarded as constituting binding international law. As a result, States with no particular interest in, or even those benefiting from, this legal vacuum are inclined to reject the notion that cyber operations particularly latent ones amount to violations of sovereignty. This underscores that international law is still in its formative stage in developing effective cyber norms, and highlights the necessity of global political will to establish binding international legal instruments applicable to all States, thereby ensuring that latency in cyber operations can no longer serve as a loophole to evade accountability for sovereignty violations. (Akbar, 2024)

It can be concluded that contemporary international law has not yet fully addressed the latency of cyber operations as a form of violation of State sovereignty. This is due to the absence of universally binding legal instruments, the inherent difficulties of attribution, the lack of consensus regarding the boundaries of digital sovereignty, and the limited capacity of international institutions to enforce State responsibility in cyberspace. These shortcomings underscore the pressing need to reform the international legal system so that it becomes more adaptive and responsive to increasingly complex and concealed digital threats. In the long term, the international community must establish a binding global cyber law convention, supported by credible investigative and adjudicative mechanisms. Without concrete progress toward such an instrument, latency in cyber operations will remain a systemic weakness of international law, readily exploited by States or malicious actors to infringe upon the sovereignty of other States with impunity.

Only through robust international collaboration and the development of specific legal regulations can the principle of sovereignty be safeguarded and remain relevant in the digital era marked by uncertainty and unprecedented challenges.

IV. CONCLUSIONS

The discussion on the impact of cyberattack latency on the principle of sovereignty from the perspective of international law demonstrates that latency in cyber operations namely, the temporal gap between the initial infiltration and the subsequent detection of its effects or the presence of the attack has created profound challenges for the effective application of the principle of State sovereignty, which has long served as a cornerstone of the international legal order. Latency not only complicates the processes of identifying an attack and attributing responsibility to either State or non-State actors, but also undermines the victim State's capacity to respond promptly and lawfully through legal or diplomatic measures aimed at safeguarding its territorial integrity and jurisdiction. In such circumstances, the principles of non-intervention and the prohibition on the use of force, enshrined in the United Nations Charter, become increasingly difficult to enforce, particularly where no immediate physical damage can be demonstrated within a short period of time. Moreover, the absence of binding international consensus on the delineation of cyberspace as part of sovereign territory, the inadequacy of international legal instruments specifically governing cyber operations, and the lack of an effective global enforcement mechanism against violations in the digital domain collectively indicate that contemporary international law has yet to fully address the latent dynamics of increasingly sophisticated and concealed cyberattacks. Consequently, the latency of cyber operations substantially weakens the protection of State sovereignty and expands the space for impunity enjoyed by perpetrators in cyberspace. This situation underscores the urgent need for the progressive development of international law through the establishment of new norms, binding global conventions, and collaborative as well as adaptive enforcement mechanisms capable of responding to the challenges of the digital era.

REFERENCES

1) Akbar, R. S. (2024). Bela Negara Di Era Digital : Tantangan Dan Strategi Memperkokoh Nilai-Nilai Kebangsaan Melalui Teknologi. *INNOVATIVE:* Hubungan *Journal Of Social Science Research*, 8418-8428.
2) Marzuki, P. M. (2005). *Penelitian Hukum.* Jakarta: Prenadamedia Group.
3) Maskun. (2020). *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional.* Makassar: CV. Nas Media Pustaka.
4) Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika: Media Hukum dan Keadilan* .
5) Noor, J. (2011). *Metodologi Penelitian.* Jakarta: Kencana Prenada Media Group.
6) Prasetyo, M. J. (2023). Pemberlakuan Prinsip Kedaulatan Wilayah Menurut Hukum Internasional Sebagai Unsur Berdirinya Negara. *Lex Administratum*, 35-45.
7) Puspita, N. Y. (2022). Rekonseptualisasi Prinsip Kedaulatan Negara Dalam Penanggulangan Bencana Di Indonesia: Pelajaran Dari Covid-19. *Jurnal Arena Hukum*.
8) Putra, R. D. (2018). Siber threats instate defense persfectives (Total Defense System Case Study). *Jurnal Prodi Perang Asimetris*.
9) Rachman, A. M. (2021). Implikasi Prinsip Right Of External Self Determination Terhadap Kedaulatan Negara Induk Sebagai Subjek Hukum Internasional . *Jendela Hukum*, 48-51.
10) Radsan, J. (2007). The Unresolved Equation of Espionage and International Law. *Michigan Journal of International Law*, 597.
11) Satjipto Rahardjo, d. A. (2004). *Hukum dan Penelitian Hukum.* Bandung : Citra Aditya Bakti.
12) Yanuar, A. P. (2021). Cyber War: New National and International Security Threat. *Jurnal Keamanan Nasional*, 23-35.

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