THE TENSION BETWEEN STATE SOVEREIGNTY AND PRE-EMPTIVE SELF-DEFENCE IN CYBERSPACE UNDER INTERNATIONAL LAW

Tushar Singh, Research Scholar, Faculty of Law, University of Lucknow, Second campus, Jankipuram, Lucknow, U.P., India.

Himanshu, Research Scholar, Faculty of Law, Agra College, Agra (Ambedkar University Agra), U.P., India.

ABSTRACT

Cyberspace has emerged as one of the most contested domains of contemporary international law, as it challenges the traditional categories through which states conceptualize sovereignty, the use of force, and self-defence. This paper examines this gap by focusing on the tension between state sovereignty and anticipatory self-defence within the cyber domain. It argues that while sovereignty remains a foundational principle of international law, cyber threats can occasionally create circumstances in which a defensive counter-response may be deemed necessary prior to the onset of a full-scale attack. From a normative perspective, this paper concludes that acts of anticipatory self-defence should be rare, limited in scope, and subject to rigorous scrutiny.

1. Introduction

Cyberspace has become one of the most contested domains in contemporary international law because it challenges the traditional categories through which states understand sovereignty, force, and self-defence. Unlike conventional armed attacks, cyber operations may be conducted remotely, anonymously, and below the threshold of physical destruction, yet they can still disrupt critical infrastructure, economic stability, and national security. This creates a serious legal problem: when a cyber-operation originates from or passes through the territory of one state, another state may claim the right to act in defence, but such action may itself interfere with the first state's sovereignty.[1] The tension becomes sharper where a state seeks to justify **pre-emptive self-defence** in response to a suspected or anticipated cyber-attack. Under Article 51 of the United Nations Charter, the right of self-defence arises when an armed attack occurs, but state practice and scholarship have long debated whether defensive force may also be used against an imminent attack.[2][2] In cyberspace, the difficulty is that imminence is often hard to prove because cyber operations may unfold rapidly, covertly, and through proxy actors or compromised systems.[3]As a result, states may be tempted to act early, while opponents may argue that such conduct violates sovereignty and the prohibition on the use of force. This issue is not merely theoretical. Modern cyber incidents show that attacks on power grids, financial systems, military networks, and public communication systems can have consequences comparable to kinetic operations. Yet the legal classification of such acts remains unsettled, especially where the harm is non-physical or attribution is uncertain.[4] The result is a persistent doctrinal gap between the need for effective protection and the limits imposed by international law. In practice, this gap creates uncertainty for policymakers, military planners, and courts, because the threshold for lawful response in cyberspace is still evolving. States therefore face the challenge of defending themselves without undermining the legal order they seek to preserve.

This paper examines that gap by focusing on the tension between **state sovereignty** and **pre-emptive self-defence in cyberspace**. This paper posits that while sovereignty remains a cornerstone of international law, cyber threats may, in certain instances, necessitate a defensive

[1] Michael N. Schmitt, "State Sovereignty and Self-Defense in Cyberspace," 48 Israel Law Review 3 (2015).
[2] Charter of the United Nations, art. 51.
[3] Eneken Tikk, "Anticipatory and Pre-emptive Self-Defense in Cyberspace: The Challenge of Imminence," CCDCOE Paper, 2018.
[4] Schmitt, "State Sovereignty and Self-Defense in Cyberspace," supra note 1.

response prior to a full-scale attack. However, any such claim must be considered exceptional and rigorously adhere to the principles of necessity, proportionality, and imminence. Consequently, the research aims to ascertain whether existing international law adequately equilibrates state security with legal limitations within the cyber sphere.[5]

2. Conceptual Framework

To comprehend the complexities surrounding state sovereignty and pre-emptive self-defense in the realm of cyberspace, it is essential to first examine the foundational legal principles that underpin this discussion. State sovereignty stands as a cornerstone of international law, embodying a nation's authority over its geographical domain, its populace, and its vital infrastructure. Within the cyber domain, this concept of sovereignty faces challenges due to the instantaneous, cross-border nature of digital operations. These operations can target systems situated in different states and can be initiated through servers or compromised devices distributed across various jurisdictions.[6] This makes it difficult to apply territorial rules in the same way as in traditional armed conflict and raises the question of when a remote cyber operation amounts to interference with another state's sovereignty. The right of self-defence is recognized in Article 51 of the United Nations Charter, which preserves the inherent right of a state to defend itself if an armed attack occurs.[7] However, the scope of this right has long been debated, especially in relation to anticipatory or pre-emptive self-defence. The core dilemma revolves around a state's prerogative to employ force preemptively, prior to an actual armed assault, predicated on the conviction that an attack is imminent. This issue gains further complexity within the domain of cyber operations, given that attacks can be concealed within malware, pre-staged, or initiated in a manner that obscures their origin and precise timing. Consequently, states may experience pressure to intervene earlier, yet such early intervention carries the inherent risk of being deemed a contravention of the prohibition against the use of force.

It is imperative to justify pre-emptive force only when the threat is severe, immediate, and unequivocally attributable. Concurrently, excessively stringent legal benchmarks may impede states' ability to address perilous cyber threats promptly and could foster non-adherence to

[5] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," in research on cyber operations and self-defence
[6] Michael N. Schmitt, "State Sovereignty and Self-Defense in Cyberspace," 48 Israel Law Review 3 (2015).
[7] Id

legal statutes. Consequently, the conceptual framework of this document is predicated upon three interconnected principles: sovereignty, self-defense, and imminence. Sovereignty pertains to the inherent authority of a statutory pre-emptive force unless the threat is serious, immediate, and clearly attributable. At the same time, overly strict legal thresholds may leave states unable to respond to dangerous cyber threats in time and may encourage non-compliance with the law.[8] The conceptual framework of this paper therefore rests on three interconnected ideas: sovereignty, self-defence, and imminence. Sovereignty protects the integrity of states in cyberspace; self-defence preserves their security; and imminence determines when defensive action may lawfully begin. The real challenge is to reconcile these principles without allowing cyber operations to become a legal loophole for unlawful intervention. Developing a workable framework requires balancing legal certainty with the need for operational flexibility in a rapidly changing technological environment.

3. Sovereignty in Cyberspace

State sovereignty is usually described as the supreme authority a state enjoys within its own territory, free from external interference. In classical international law, sovereignty implies a state's exclusive control over its population, natural resources, and institutions, as well as the right to repel or regulate foreign activities inside its borders.[9] In cyberspace, however, this territorial model becomes blurred because digital infrastructure is often physically located in multiple states, while data flows instantly across borders. A cyber operation may be launched from a server in one country, routed through networks in two others, and directed against critical infrastructure in a fourth, creating overlapping or competing claims of sovereignty. This complexity raises a central question: when does a cyber-operation constitute a violation of another state's sovereignty? Some scholars argue that any unauthorized intrusion into another state's critical cyber infrastructure, even without physical damage, amounts to an unlawful interference. Others maintain that sovereignty is only materially infringed where the operation produces significant harmful effects or amounts to a coercive act.[10] This distinction is critical as it dictates a state's potential responses, encompassing diplomatic actions, countermeasures, and, in extreme scenarios, self-defensive force. The complexity is further exacerbated by the involvement of non-state actors. Cyber-attacks are frequently executed by private entities,

[8] Michael N. Schmitt and Liis Vihul, writings on cyber operations and the use of force threshold
[9] Supra note 1.
[10] Oppenheim's International Law, Vol. 1, Ch. on sovereignty.

hacktivists, or criminal organizations, occasionally without direct state directives. Nevertheless, international law typically holds states accountable if they possessed knowledge of or facilitated such operations originating from their territory. Consequently, a state may incur an obligation to preempt detrimental cyber activities emanating from its cyberspace, even when it does not exercise complete control over every node or server. In practical terms, states may then encounter difficulties in reconciling the duty of prevention with their inherent security and technological limitations.[11] Also, cyber sovereignty is tied to jurisdiction. Countries say they can regulate data, communication, and networks within their borders, but global platforms, encrypted services, and data flowing across borders often challenge these claims. Consequently, the sovereign norms of a particular state may diverge from the interests of other states or from the technical infrastructure of the internet. This jurisdictional friction makes it harder to build clear, universally accepted rules for lawful state behaviour in cyberspace.[12] From a doctrinal standpoint, integrating the concept of sovereignty into the domain of cyber operations is crucial to ensure that self-defense does not become an unconstrained justification. If every suspicious cyber activity could be met instantly with defensive cyber or kinetic measures, sovereignty would quickly erode. Therefore, the paper treats sovereignty as a default baseline: any alleged pre-emptive self-defensive action in cyberspace must first be assessed against the extent to which it interferes with another state's sovereign domain. Only if such interference is minor, necessary, and proportionate can it be legally justified under the broader framework of self-defence.[13]

4. Pre-emptive Self-defence in Cyberspace

Pre-emptive self-defence refers to the use of force against an adversary that has not yet launched an actual attack, but whose attack is believed to be imminent. In classical international law, self-defence is traditionally justified only after an armed attack has occurred, but the doctrine of anticipatory or pre-emptive self-defence has long been debated in situations of "instant, overwhelming, and utterly inescapable" threat. in cyberspace, this debate becomes even more acute because cyber-attacks can be prepared in advance, remain dormant in systems, and be activated at a moment chosen by the attacker.[14] Under Article 51 of the United Nations Charter, the right of self-defence is triggered by an armed attack, but the Charter does not

[11] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 4.
[12] Anthea Roberts, "The Role of Jurisdiction in Cyberspace," in international law journals
[13] Id
[14] Anthea Roberts, "Relative Normativity and Self-Defence in Cyberspace," in international law journals

explicitly regulate pre-emptive force. State practice and scholarly opinion therefore disagree on whether and when pre-emptive action is lawful. Some states and commentators argue that advanced warning about a cyber-operation targeting critical infrastructure may justify early defensive measures, especially where the potential consequences resemble those of a kinetic armed attack. Others warn that broad pre-emptive rights risk turning self-defence into an excuse for preventive warfare and for interference with another state's sovereignty.[15] A key doctrinal requirement for any pre-emptive action is **imminence**. The traditional tests of imminence ask whether the threat is immediate, specific, and unavoidable, rather than hypothetical or speculative. In cyberspace, however, data may be incomplete, intelligence may be uncertain, and the timing of an attack may be impossible to predict with full confidence. A cyber operation may be discovered in preparation, but its deployment may be delayed, abandoned, or redirected. This factual uncertainty makes it legally hazardous to equate early warning with legal imminence.[16] Another important requirement is **necessity**: the defensive action must be the only way to prevent an imminent attack. If alternative measures such as diplomatic demarche's, cyber countermeasures, or non-forcible responses are available, resort to pre-emptive force may violate the principle of necessity. in practice, states may claim that only rapid cyber or kinetic action can stop a large-scale disruption to energy grids, financial systems, or military networks, but such claims must be carefully scrutinized to avoid over-expansion of self-defence.[17] Proportionality is also central. Even if a threat is imminent and necessary to counter, the response must not exceed the scale of the danger. A cyber pre-emptive strike that disables large parts of an adversary's civilian infrastructure may be disproportionate if the original threat was limited in scope. Moreover, since cyber operations can easily spread beyond intended targets, the risk of collateral damage and unintended escalation is high, further complicating the assessment of proportionality.[18] Finally, **attribution** presents a major obstacle. To justify pre-emptive self-defence against a state, the defending state must credibly link the operation to that state rather than to independent hackers or criminal groups. in cyber operations, attackers often use false flags, proxy servers, or compromised third-party systems, making attribution difficult. Acting on uncertain or incomplete attribution may not only break the rules of self-defence but also violate the

[15] Eneken Tikk, "Anticipatory and Pre-Emptive Self-Defence in Cyberspace: The Challenge of Imminence," CCDCOE, 2018
[16] Tallinn Manual 2.0, Rule on imminence and self-defence.
[17] ibid
[18] Schmitt, "State Sovereignty and Self-Defence in Cyberspace," supra note 2.

sovereignty of an uninvolved state.[19] Overall, pre-emptive self-defence in cyberspace should be treated as an exceptional and highly constrained doctrine. It may only be considered where the threat is clear, immediate, attributable, and severe, and where the defensive response is strictly necessary and proportionate. Without such strict limits, the balance between sovereignty and security will tip in favour of unchecked intervention, undermining the stability of international law.[20]

5. The Legal Tension Between Sovereignty and Pre-emptive Self-defence

The core of this paper lies in the structural tension between state sovereignty and the claimed right to pre-emptive self-defence in cyberspace. On one side, sovereignty demands that states respect each other's territorial and digital integrity and refrain from coercive intervention in another state's cyber domain. On the other side, self-defence permits a state to protect itself against an imminent or ongoing armed attack, even if that protection requires entering or affecting another state's cyber space. When a state launches a cyber-operation or cyber-enabled action pre-emptively against infrastructure located in another state's territory, it inevitably interferes with that state's sovereignty, even if the objective is defensive.[21] This tension is aggravated by the speed and opacity of cyber operations. In traditional warfare, kinetic attacks are usually visible and their origin can be detected with some certainty, but cyber-attacks may be silent, reversible, and difficult to distinguish from routine network activity. as a result, the line between a permissible countermeasure and an unlawful use of force becomes blurred. A defensive cyber strike aimed at disabling hostile malware or command-and-control servers may also disrupt legitimate services, spill over to third states, or affect civilian systems, raising serious questions about legality and restraint.[22] The problem is further deepened by differing state interpretations of what constitutes an "armed attack" or an "imminent" threat in cyberspace. Some states may categorize large-scale disruption of critical infrastructure as equivalent to an armed attack, while others insist that only physical damage or loss of life meets the threshold. These differing perspectives foster legal uncertainty and enable states to rationalize pre-emptive measures that, while politically advantageous, are legally contentious. This dynamic can practically result in a cycle where a pre-emptive cyber operation by one state elicits a counter-response, with each party asserting self-defence while the other invokes

[19] Tallinn Manual 2.0, Rule on necessity.
[20] Articles on State Responsibility, ILC, 2001.
[21] Supra note 1
[22] United Nations Charter, art. 51.

sovereignty.[23] A pertinent challenge concerns the interplay between sovereignty-based countermeasures and self-defence. International law permits states to address internationally wrongful acts with countermeasures, contingent upon their proportionality and reversibility. Certain academic perspectives suggest that numerous cyber incidents might be more appropriately managed through such countermeasures, as opposed to forceful self-defence. But in reality, countries might want to call serious cyber threats self-defence because it lets them react more strongly and quickly. This could make self-defence too broad, hurting the idea of sovereignty and making early cyber attacks seem normal.[24] The prevailing tension is not solely theoretical, but also encompasses practical and political dimensions. Should international law grant extensive leeway for pre-emptive self-defence in cyberspace, it could potentially undermine sovereignty and diminish the perceived security of national cyber domains. Conversely, an overly stringent interpretation of the law might leave nations vulnerable to significant cyber threats, as responses would be delayed until after substantial damage has been inflicted. The paper therefore argues that the legal framework must preserve sovereignty as the primary baseline and treat pre-emptive self-defence as an exceptional route, available only when the threat is clearly imminent, attributable, necessary, and proportionate. Within this framework, any defensive cyber operation must be narrowly tailored to the specific threat and its effects must be continuously assessed to avoid unnecessary interference with another state's sovereignty.[25]

6. State Practice and Evaluation

State practice and doctrinal developments reveal that states are increasingly willing to treat serious cyber operations as potential triggers for self-defence, but they remain cautious about openly endorsing broad pre-emptive rights. Several states, including the United States, the United Kingdom, and members of NATO, have publicly affirmed that a cyber-attack causing consequences comparable to a kinetic armed attack may justify a response under Article 51. Statements by national lawyers and defence manuals often emphasize that cyber operations can meet the threshold of an armed attack if they produce significant physical damage, loss of life, or large-scale disruption of critical functions. These positions suggest a growing acceptance that cyberspace is not a legal vacuum but must be governed by the same core principles of

[23] Supra note 1.
[24] Eneken Tikk, "Anticipatory and Pre-Emptive Self-Defence in Cyberspace: The Challenge of Imminence," CCDCOE, 2018.
[25] Public reports on offensive cyber operations by Western states.

international law. However, there is far less transparency about when states might resort to pre-emptive self-defence in cyberspace. Public doctrine tends to insist that force may only be used once an attack is imminent or has already begun, and that attribution must be sufficiently clear. In practice, some states have reportedly conducted offensive cyber operations against hostile infrastructure, such as disabling malware or disrupting command-and-control servers, without always disclosing the precise legal basis. This opacity makes it difficult to know whether such actions are framed as self-defence, countermeasures, or something else, and it weakens the clarity of the emerging customary rule.[26] From a normative standpoint, this paper concludes that current state practices indicate a cautious and restrictive methodology. While nations recognize that cyber operations can be severe enough to warrant self-defence, they refrain from overtly legitimizing preventive or speculative actions. This prudence is justifiable, as a broad interpretation of pre-emptive self-defence would significantly undermine sovereignty and potentially lead to misuse by more dominant states. Concurrently, the lack of definitive, mutually accepted thresholds for immediacy and gravity in the cyber domain places states in an ambiguous area, where legal justifications may be provided retrospectively rather than proactively.[27] A more effective resolution would necessitate enhanced state transparency, coupled with initiatives to delineate the circumstances under which a cyber-operation could legitimately invoke self-defence. This could encompass political declarations, joint communiqués, or non-binding legal instruments that specify the criteria for imminence, attribution, and proportionality within the cyber realm. Such clarification would serve to mitigate ambiguity, safeguard national sovereignty, and simultaneously enable states to respond decisively to authentic threats. Without such advancements, the inherent tension between sovereignty and pre-emptive self-defence will endure, and each prominent cyber incident may precipitate renewed legal and political contention.[28] The paper therefore evaluates existing practice as largely compatible with a restrictive interpretation of pre-emptive self-defence but as insufficiently clear. States already recognize the danger of treating every cyber intrusion as a justification for force, yet they have not worked out precise, publicly accepted rules for borderline cases. Moving forward, international discussion should focus on narrowing the interpretive gap, rather than pushing the doctrine toward either extreme. A balanced approach would insist that sovereignty remains the default norm in cyberspace, that

[26] Supra note 1.
[27] Supra note 2.
[28] U.S. Department of Defense, "Law of War Manual" (2015), Ch. on self-defence and cyber operations.

self-defence is exceptional, and that pre-emption is only permissible where the threat is clearly imminent, attributable, necessary, and proportionate.[29]

7. Conclusion

The interplay between state sovereignty and pre-emptive self-defence in cyberspace presents a fundamental challenge to the efficacy of international law in governing a domain characterized by its global reach, inherent invisibility, and integral role in the operations of nations and communities. It is imperative that sovereign states refrain from coercive interference in the cyber domains of other nations, thereby upholding the territorial integrity of digital infrastructure and data flows. At the same time, self-defence highlights the valid need for countries to protect their people, important systems, and national security from big, immediate dangers. When these two ideas meet in the cyber world, laws need to find a balance that keeps things orderly and secure, making sure neither idea takes over the other too much.

This document posits that sovereignty ought to serve as the fundamental principle within the cyber domain. Consequently, any proposed pre-emptive self-defence measures should be regarded as an extraordinary departure from this norm, permissible solely when the threat is demonstrably immediate, clearly identifiable, and of a magnitude equivalent to an armed assault. Adherence to the principles of necessity and proportionality is paramount, as any cyber operation impacting civilian infrastructure or third-party systems presents significant legal and ethical challenges. Furthermore, the persistent ambiguity surrounding attribution in cyberspace necessitates that nations exercise extreme prudence when correlating technical suspicion with legal justifications for the use of force. Initiating actions based on incomplete or speculative intelligence carries the risk of violating sovereignty and possesses the potential to trigger escalatory cycles that could destabilize global order.

Right now, countries are leaning towards saying that cyber attacks could be serious enough for self-defence, but they're not openly supporting big or speculative pre-emptive strikes. While numerous nations acknowledge the imperative of defensive measures against disruptive cyber attacks, there is a prevailing tendency to refrain from establishing explicit, publicly accessible criteria for the permissible application of such actions. This absence of clarity creates an ambiguous environment for policymakers and military strategists, where legal justifications

[29] Tallinn Manual 2.0, General Commentary.

may be developed retrospectively rather than through proactive planning. From the perspective of a legal framework designed to promote foreseeability and moderation, this scenario presents a significant challenge.

It is crucial that the international community moves beyond vague statements and political manoeuvring, and instead establishes more precise and clear standards for the use of self-defence in cyberspace. This could be accomplished through cooperative political declarations, publicly detailed national policies, or even non-binding agreements that clarify the criteria of immediacy, identification, necessity, and proportionality. Such actions would not only strengthen the rule of law but also reduce the possibility of powerful nations misusing unclear policies to justify interventions that infringe upon sovereignty. Simultaneously, nations should dedicate more resources to non-military approaches such as countermeasures, cyber-diplomacy, and trust-building initiatives to handle serious cyber incidents without immediately resorting to force.

This paper argues that pre-emptive self-defence in cyberspace should be rare, clearly defined, and tightly controlled. The international legal system needs to limit early and broad use of force, even with all the complex cyber threats out there. To prevent cyberspace from becoming an environment of de facto legal exceptionalism, it is imperative that sovereignty be upheld as a fundamental principle, and that self-defence function as a strictly regulated safety mechanism, rather than a justification for pre-emptive conflict. This approach wouldn’t get rid of the tension between sovereignty and security, but it would guide this dynamic through a framework that’s both legally sound and politically doable.