# CAN CYBER OPERATIONS AMOUNT TO AN 'ARMED ATTACK' TRIGGERING SELF DEFENCE UNDER ARTICLE 51?

**Ananya Rana*** **Ananya Rajput***

## ABSTRACT

*The emergence of cyber operations has challenged the traditional understanding of the right to self-defence under Article 51 of the United Nations Charter. This paper examines whether cyber-attacks can constitute an 'armed attack' capable of triggering a state's inherent right of self-defence. It analyses the legal framework established by Article 2(4) and Article 51 of the Charter, together with the jurisprudence of the International Court of Justice, particularly the Nicaragua case and subsequent decisions. The study argues that cyber operations may amount to an armed attack when their scale and effects are comparable to those of conventional kinetic attacks. Drawing on the Tallinn Manual 2.0, the Schmitt criteria, state practice, and the example of the Stuxnet operation, the paper evaluates the applicability of existing international law to cyberspace. It further identifies unresolved challenges relating to cumulative harm, attribution, and non-state actors, demonstrating that significant legal uncertainty continues to surround cyber self-defence in contemporary international law.*

**Keywords:** Cyber Operations, Article 51, Armed Attack, Self-Defence, International Law.

## INTRODUCTION

In 2010, malicious code destroyed about a thousand uranium enrichment centrifuges at Iran's Natanz facility. The Stuxnet worm is widely attributed to a joint United States and Israeli operation. It did, through software, what would otherwise have required a kinetic strike. Yet Iran did not invoke Article 51, and no state has formally done so over a cyber operation. That silence is the puzzle this paper takes up. Article 2(4) of the Charter prohibits the threat or use

*BBA LLB (HONS.), FOURTH YEAR, O.P. JINDAL UNIVERSITY, SONIPAT.
*BBA LLB (HONS.), FOURTH YEAR, O.P. JINDAL UNIVERSITY, SONIPAT.

of force,[1] while Article 51 preserves the inherent right of self-defense 'if an armed attack occurs.'[2] The drafters in 1945 had bombs and battalions in mind, not botnets. This paper asks whether that framework, designed for a kinetic world, can fit operations made of zeroes and ones. It argues that cyber operations *can* amount to an armed attack under Article 51, but only when their scale and effects match those of a conventional armed attack. Sections II and III set out the framework and apply it. Section IV of the paper examines its limits.

## THE LEGAL FRAMEWORK: ARTICLE 51 AND THE 'ARMED ATTACK' THRESHOLD

**The Article 2(4) Prohibition and the Article 51 Exception:** The Charter sets out a near absolute ban on the use of force. Two exceptions apply. The first is Security Council authorisation under Chapter VII. The second is self-defence under Article 51. The phrase 'inherent right' traces back to the 1837 Caroline incident, where Daniel Webster set out the canonical test that self-defensive force must respond to a necessity which is "instant, overwhelming, leaving no choice of means, and no moment for deliberation."[3] Caroline is invoked here not for the threshold question of what counts as an armed attack, which is Nicaragua's domain, but for the conditions any lawful response must meet, namely necessity and proportionality. These customary requirements survive into the Charter era and apply equally to cyberspace.

**Defining 'Armed Attack': The Nicaragua Threshold:** Article 51 does not define 'armed attack.' The International Court of Justice supplied the definition in Nicaragua (1986), holding that an armed attack is the 'most grave form of the use of force,' different from "less grave forms" such as frontier incidents or the provision of weapons to rebels.[4] This produced what is often called the Nicaragua gap, a category of unlawful uses of force under Article 2(4) that fall short of triggering self-defence.[5] The threshold is high by deliberate design, meant to stop states from dressing up retaliation as self-defence.

[1] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 2(4).
[2] ibid art 51.
[3] Letter from Daniel Webster to Lord Ashburton (6 August 1842), reproduced in British and Foreign State Papers, vol 30, 195.
[4] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 191.
[5] ibid para 195.

**Confirmation in Subsequent ICJ Jurisprudence:** The Nicaragua threshold has proved durable. In Oil Platforms, the Court reaffirmed the test and asked whether smaller incidents could be added together to meet it. It found that the missile and mining incidents alleged by the United States, even taken together, did not amount to an armed attack by Iran.[6] The Wall Advisory Opinion and Armed Activities (DRC v Uganda) applied the test in the same way.[7] Nicaragua remains the lens through which any candidate's armed attack, kinetic or digital, must be assessed.

## APPLYING THE FRAMEWORK TO CYBERSPACE. THE SCALE AND EFFECTS TEST

**Effects, Not Instruments:** The doctrinal hinge that lets cyber into the Article 51 conversation is the ICJ's pronouncement in the nuclear weapons Advisory Opinion that Article 51 applies 'to any use of force, regardless of the weapons employed.'[8] International law cares about consequences, not conduits. A power station may be destroyed by a cruise missile or by code that overrides its safety controls, and the resulting damage is legally indistinguishable. This effects-based reading is the foundation of every serious analysis of cyber and jus ad bellum.

**Operationalising the Test. The Tallinn Manual and the Schmitt Criteria:** Rule 71 of the Tallinn Manual 2.0 is the most authoritative restatement of cyber-applicable international law, prepared under the NATO Cooperative Cyber Defence Centre of Excellence. It provides that a state targeted by a cyber operation rising to the level of an armed attack may exercise self-defence.[9] To make the test workable, Michael Schmitt proposed six factors (severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy). The Tallinn International Group of Experts adopted these and added factors such as military character and degree of state involvement.[10] Severity does most of the heavy lifting. An operation producing death, injury, or significant physical destruction is presumptively an armed attack. One that merely defaces a website is not. The factors are not a checklist. They are a structured way of

[6] *Oil Platforms (Islamic Republic of Iran v United States of America)* (Merits) [2003] ICJ Rep 161, paras 64, 72.
[7] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep 168, paras 146 to 147; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136, para 139.
[8] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 39.
[9] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) Rule 71.
[10] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885, 914 to 915; Schmitt (n 9) Rule 69 commentary, para 9.

asking the obvious question, namely, whether we would still hesitate to call this an armed attack if it had been done with explosives.

**Stuxnet as the Paradigm Case:** Stuxnet remains the cleanest test of the framework. The worm caused real physical damage to nuclear infrastructure and was attributable to state actors.[11] On the Schmitt criteria of severity, directness and military character, it scores as a use of force without difficulty. Whether it crossed into armed attack territory is genuinely contested. The Tallinn experts split, with a substantial minority concluding that it did.[12] That split is itself the analytical point. If the most destructive cyber operation in modern history sits on the threshold, Iran's decision not to invoke Article 51 looks like a political choice, not a legal disability.

**Emerging State Practice and Opinio Juris:** The strongest evidence that the test now governs cyber operations comes not from courts but from states themselves. Germany, Estonia, Finland and Italy each issued formal position papers between 2020 and 2021 endorsing the view that cyber operations comparable in scale and effect to a kinetic attack can constitute an armed attack.[13] The United States articulated the same position as early as 2012.[14] Under Article 38(1)(b) of the ICJ Statute, this convergence of state practice and opinio juris is how customary international law forms.[15] Dissent persists. Russia and China have argued that Nicaragua's framework was never intended for cyberspace and have pushed for a new treaty regime.[16] The trend among states publicly addressing this is nonetheless unmistakable. The law is not waiting for a treaty. It is being written, one position paper at a time.

## CRITICAL ANALYSIS: THE UNRESOLVED GAPS

Even though we have established that cyber operations can trigger Article 51, it would not be okay to assume that this is the end of the story. Even though the framework in itself looks

[11] Margherita D'Ascanio, Marco Sassòli and Yvette Issar, *The Stuxnet Cyberattack on Iran's Nuclear Facilities: An IHL Analysis* (Geneva Academy 2025).
[12] Schmitt (n 9) Rule 71 commentary, para 10.
[13] Federal Government of Germany, *On the Application of International Law in Cyberspace* (Position Paper, March 2021); Government of Estonia, National Position, in UN Doc A/76/136 (2021); Ministry for Foreign Affairs of Finland, *International Law and Cyberspace: Finland's National Positions* (2020); Ministry of Foreign Affairs and International Cooperation of Italy, *Italian Position Paper on International Law and Cyberspace* (November 2021).
[14] Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal Online* 1, 4.
[15] Statute of the International Court of Justice, art 38(1)(b).
[16] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan to the United Nations Secretary General, 'International Code of Conduct for Information Security' UN Doc A/69/723 (13 January 2015).

coherent in theory, it begins to unravel when applied to how cyber operations work practically. The once clear threshold becomes tricky to locate in reality. Three continuous gaps complicate it. Each of them exposes how there is a severe mismatch between what is assumed by the law and what is operated by cyberspace.

**Gap 1: Continuous Harm:** The most structural difficulty in this aspect is the fact that cyber harm never appears as a single or decisive event. As developed in the case of Nicaragua vs United States, the scale and effects test were made for discrete acts such as missiles striking targets or troops crossing the borders.[17] Cyber-attacks operate on a different tangent in themselves. They are majorly persistent, and on top of that, they are also incremental in nature. They are also calculated in a way that they remain below the threshold of an 'armed attack' while also imposing real harm. This gives rise to the problem of 'death by a thousand cuts'. Contemporary cyber strategies frequently rely on low-risk intercept able operations like intellectual property theft, interference with the election, etc. Ordinarily, these acts will not come under the threshold of Article 51. But it becomes very easy for the same acts to erode a country's economic stability, democratic processes and national security if done collectively for a long period of time. This is not just a theoretical concern. Industry analysis describes modern cyber risk as something that consists of frequent, low-intensity disruptions like system outages, communication failures and data interruptions. These acts "trickle into significant aggregates of wastage and unnecessary costs" instead of being a singular dramatic event.[18] From this understanding, cyber harm operates in a continuous process of degradation.

This challenge is also acknowledged in the Tallinn Manual 2.0. It notes that a series of cyber operations can be assessed collectively under the "accumulation of events" approach.[19] However, it does not give a clear criterion when this accumulation crosses a threshold, while state practice remains limited. An example of this ambiguity is incidents like the 2007 Estonia DDoS attacks and the 2015-16 Ukrainian power grid disruptions. Through this, international law appears ready to regulate force rather than the slow, calculated harms that increasingly define cyber conflict.

[17] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)* (Merits) [1986] ICJ Rep 14.
[18] CyberOwl, 'Death by a Thousand Cyber Cuts' (2021) https://cyberowl.io/death-by-a-thousand-cyber-cuts/ accessed 2 May 2026.
[19] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) r 71 commentary.

**Gap 2: The Attack Without an Attacker:** If one were to overcome the first problem, a second, more fundamental problem emerges. Self-defence presumes that the victim state can identify the attacker. This assumption becomes deeply fragile. Cyber operations are very much capable of causing harm without any physical presence. They are also designed to be uncertain from their origin through proxy routing, spoofing, botnets and false flag operations. International law has a demanding standard of attribution. Under the Articles on state responsibility (ARSIWA), a state's conduct is attributable where it is carried out by state organs or by non-state actors who act under its instruction, direction or control.[20] In the Nicaragua case, the ICJ articulated the "effective control" test, which requires a high degree of state involvement.[21] Although the ICTY in the case of Prosecutor vs Tadic suggested a broader "overall control" test, the ICJ in the case of Bosnia vs Serbia rejected this test and confirmed a stricter standard for attributing state actions.[22] This creates a near paradox in the context of cyber-attacks. The "effective control" test makes a presumption that the attacker can be reliable and identifiable. Cyber operations are specifically made to prevent this from happening. An example for this is the 2007 Estonia attacks, where it was subjected to three weeks of DDoS attacks which targeted governmental, financial and media websites.[23] Even though it did contribute widely to political discourse, it was never established legally. This gap showcases that, practically, cyber operations remain outside the reach of a lawful self-defence.

**Gap 3: When the Threat is not a State:** The problem is further deepened when the attacker is clearly not the state. Cyber operations are carried out by many non-state actors, like hacker groups, criminal networks, etc. Their relationship with the state is ambiguous. But can Article 51 be invoked when the attack is not directly attributable to a state? Post 9/11 developments showcase a partial opening. UN Security Council Resolutions 1368 and 1373 recognised that non-state actors can carry out attacks of sufficient gravity to trigger self-defence.[24] However, the ICJ's Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory appeared to reintroduce a requirement of state involvement, thereby creating doctrinal

[20] International Law Commission, 'Articles on Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/56/10 arts 4–11.
[21] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)* (Merits) [1986] ICJ Rep 14 [115].
[22] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 43.
[23] Michael N Schmitt and Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014) 1 *Fletcher Security Review* 55.
[24] UNSC Res 1368 (12 September 2001) UN Doc S/RES/1368; UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373.

uncertainty.[25] The unwilling doctrine remains contested. States like the United States, the United Kingdom and Australia argue that force may be used in another state's territory if that state cannot address the threat.[26] However, scholars from TWAIL criticise this approach as it is applied inconsistently and undermines sovereign equality.[27] In cyberspace, the issue becomes even more complex: harmful activity often originates from states that lack the capacity to control it rather than those that actively support it. This blurs the line between inability and unwillingness, making it difficult to justify the use of force. As a result, the doctrine continues to generate significant legal uncertainty.

## CONCLUSION

By looking at these gaps, it becomes clear why yes is not the full answer to our question. Cyber operations may trigger Article 51 when they are similar to other kinetic attacks. But this standard in itself is uncertain in nature. Despite all the examples mentioned in this paper, no state has formally invoked Article 51. This suggests that there is a clear preference for strategic ambiguity over a proper binding precedent. This results in the framework adapting rather than failing, but most of the cyber activity still falls in the grey area.

[25] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136.
[26] Daniel Bethlehem, 'Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors' (2012) 106 *American Journal of International Law* 770.
[27] Ntina Tzouvala, 'TWAIL and the "Unwilling or Unable" Doctrine' (2015) 109 *American Journal of International Law Unbound* 266.