The Legal Boundaries of Cyber Warfare

Wynnie Yusi Feng[1, a]

[1]School of Law, Peking University, Beijing, China

[a]wynniefeng1128@gmail.com

Abstract

Although cyber operations have emerged as a key weapon in contemporary state conflicts, it is still unclear which legal frameworks apply to them. Cyberwarfare is not specifically addressed by traditional international law, such as the United Nations Charter, which was created with traditional military force in mind. Consequently, a large number of cyberattacks that actually cause harm fall into grey areas. This paper identifies the primary legal and practical issues while investigates the application of international law to cyber operations. It looks at three theories—the tool theory, the target theory, and the effect theory—that define "use of force" in cyberspace. The main obstacles to enforcement are also covered in the paper, such as issues with attribution, accountability, and impact assessment. To illustrate how these problems appear in real life, the Stuxnet attack on Iran's nuclear facilities serves as a crucial case study. The findings highlight the extent to which existing legal standards lag behind the evolving nature of contemporary threats. There is an urgent need for enhanced international cooperation, harmonized definitions, and the development of more precise regulatory frameworks.

Keywords

Cyber Warfare; International Law; Stuxnet; Use of Force; Tallinn Manual.

1. Introduction

Cyberwarfare has become a major problem in the constantly evolving field of international security, making it harder to distinguish between traditional forms of conflict and cyberspace. Article 2(4) of the United Nations Charter prohibits states from threatening or employing force against the territorial or political sovereignty of other states. However, the UN Charter, which was written after World War II, did not foresee the rise of cyberwarfare, which can cause serious damage without the use of conventional military force [1]. Cyberattacks that were believed to be initiated by specific states have caused significant disruption and real-world damage over the last ten years. However, it is not evident that these attacks were in breach of any laws. Legal scholars and practitioners have differing opinions about what constitutes a "use of force" in cyberspace due to the ambiguity surrounding this concept.

The paper argues that existing international frameworks are not sufficiently specific to effectively regulate cyberwarfare. Because cyber tools are borderless and often difficult to track, it is challenging to categorise attacks as conventional "uses of force." After describing the current legislation and its boundaries, we go into detail about the three main conceptual approaches to define cyber force—the "tool," "target," and "effect" theories. The practical issues that hinder the application of the law are then addressed, including attribution, accountability, and impact assessments. In order to highlight ambiguities and demonstrate how various cyber operations bypass legal standards, the Stuxnet case—one of the most significant cases in cyberspace—will be examined using these theories.

2. International Law Frameworks and Cyber Limits

2.1. UN Charter and the “Use of Force”

Legal restraints on force are based on the UN Charter, where Article 2(4) prohibits states from threatening or using armed force against one another, with the exception of self-defense or Security Council authorisation. However, states typically apply 2(4) by analogy because cyber is never mentioned in the UN Charter. The key issue is where a digital intrusion lies on the spectrum between firing bullets or missiles and strictly economic measures, which are not covered by Article 2(4). A Chatham House report states that any cyber operation that results in harm, death, or the destruction of objects may be considered an armed attack or even the use of force [2]. Yet according to the same report, "the vast majority" of state cyber operations continue to fall below that cutoff, involving low-level intrusions that have little to no real impact. In actuality, only the most serious cyberattacks qualify as physical assaults.

The reality that no one has agreed on the threshold constitutes a significant limitation. The line at which cyber operations qualify as force "remains unsettled," according to the 2017 Tallinn Manual 2.0, an expert study (not a treaty) [3]. To arrive at a consensus, the Tallinn Manual's analysis enumerates a number of non-exhaustive factors: whether an operation is considered forceful depends on its severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, attacker's identity, and target nature. A "scale and effects" test has been adopted by many governments; Australia, Finland, Germany, the Netherlands, and New Zealand have all stated publicly that they consider the total impact of a cyber event. There isn't a single international rule because even these "effects-based" standards differ from state to state. In essence, states weigh factors "case-by-case" and believe that "no one factor is determinative." Every significant cyber incident will spark discussions about whether it "rises to the level of a use of force" until states codify criteria.

2.2. Other Legal Norms

With the exception of Article 2(4), international law provides some direction but no easy answers. The principle of sovereignty implies that foreign cyber intrusions violate a state’s territorial integrity or political independence [4]. There is disagreement, though, over whether any unauthorised cyber access violates sovereignty or just those that have a certain impact. The non-intervention rule has long been accepted as the standard. It forbids coercive actions that hinder a state's "free will" in its internal affairs; however, it is unclear if a disruptive cyberattack qualifies as coercive in that context. In general, international humanitarian law only comes into play when there is an armed conflict. IHL's rules on targeting and proportionality only apply in a few hypothetical situations because states have not yet formally declared any cyberwar (not even Stuxnet was declared a "war"). As long as there is no use of force or prohibition of intervention, cyber espionage—hacking for intelligence—is not inherently illegal under international law.

The Tallinn Manual 2.0, a set of draft regulations created by international legal experts, is the most established attempt to modify current law. It represents what the 2016 expert panel thought the law was, but it is not legally binding. Importantly, the Tallinn Manual itself emphasises that it is neither a new law nor a treaty: "it must be understood only as an expression of the opinions of the [experts] as to the state of the law" [5]. To put it another way, the Tallinn Manual 2.0 restates the law as agreed upon by the experts. While the Manual's conclusions tend to be conservative, many rules remain unresolved, even among its authors. For instance, Rule 71 stipulates that the victim may only use self-defence if the cyberattack is considered a "armed attack," while Rule 69 basically restates the ambiguity by listing the previously mentioned criteria for determining the use of force[6].

In conclusion, for the majority of cyber uses of force, no explicit treaty or accepted norm exists at present. Since their application is controversial and ambiguous, the UN Charter and conventional principles apply in general terms. Unlike international arbitration, states have generally handled cyber intrusions as a matter of their policies. This legal ambiguity motivates conceptual theory research and emphasises the need for more precise regulations.

3. Theories of Cyber "Use of Force"

Various perspectives on cyber operations have been put forth by scholars and practitioners. The tool theory, target theory, and effect (or consequence) theory are the three main theories that are frequently brought up. These theories provide different approaches to determining whether a cyber operation qualifies as a use of force for purposes of Article 2(4).

3.1. Tool Theory

According to this perspective, cyber tools (servers, code, networks) are basically tools or weapons, like a drone or missile. A data packet is not unique on its own; its use is what matters. The fact that a piece of code travelled through a computer network instead of a barrel or a rocket is therefore legally insignificant; if it causes harm comparable to that of a bomb or missile, it should be considered a use of force. This theory, in essence, is against making a clear distinction between "digital" and "physical" weapons. Those in favour claim that cyber is just another tool, just as an aeroplane can drop a bomb or a spy plane can loop with an EMP device.

3.2. Target Theory

Target theory, on the other hand, is more concerned with what is assaulted than with how. The cyber operation should only be considered a use of force if it aims at a target that is typically associated with force, such as critical infrastructure or military systems. According to this perspective, the target (a nuclear facility) is similar to a military objective, so hacking a nuclear centrifuge (as in Stuxnet) might be adequate. However, a civilian social media site or a stock exchange might not be considered a target, because these systems are not instruments of force. According to target theory, cyberattacks against specific sensitive targets are presumed to be forceful, while others are not. One drawback is that, if challenged, states may classify nearly anything as vital, giving the impression that it is arbitrary.

3.3. Effect Theory

This perspective examines the effects of the cyberattack. A computer operation is considered a use of force if it results in outcomes that are similar to those of an armed attack. The Tallinn Manual and numerous national policies implicitly support this approach. Factors like severity, directness, invasiveness, and measurability of effects are listed in the Manual's commentary. Essentially, the question is: did the cyber operation result in injury, destruction, or other significant harm? For example, if one adheres to effect theory, Stuxnet should be considered a use of force because it physically destroyed Iranian centrifuges and postponed Iran's nuclear programme. On the other hand, the SolarWinds hack obviously fails to meet effect theory's requirements for force because, despite its scope, it did not result in any physical harm or loss of functionality.

One benefit of effect theory is that it links legal decisions to observable results. It can be disputable, though, as two states may have the same physical effect, and one may define it as force while the other does not, resulting in differing interpretations.

In the end, the majority of analysts consider these theories to be complementary. In fact, Rule 69 of the Tallinn Manual 2.0 does not select a single theory; rather, it combines elements of target-based reasoning with factors similar to "effect theory." Many states openly state that the use-of-force prohibition is only triggered by cyber operations that have "scale and effects"

comparable to armed attacks, suggesting that the growing consensus in practice leans towards an effects-based standard. However, these evaluations are still subjective because "scale and effects" are not defined by any treaty. In any case, there is a commonality among the three strategies: cyber force does not necessarily require actual firearms. To put it briefly, states have not agreed on a single classification system for cyberattacks, and the classification of a cyberattack is frequently determined by the theory or combination of factors that the court or UN body uses.

4. Practical Obstacles: Attribution, Accountability, Assessment

4.1. Attribution

Proving the identity of the person behind a cyber operation is very difficult. Technical attribution depends on intelligence and forensics, but skilled attackers conceal their identities with anonymisation, false flags, and proxies. According to international law, only a state (or a non-state whose actions can be attributed to a state) may be held legally responsible. According to the International Law Commission's Articles on State Responsibility (adopted into the Tallinn Manual 2.0), the state is responsible for the actions of its organs, while non-state actors are only accountable for their actions if they were carried out in response to the state's "instructions, direction, or control" [7]. However, establishing that causal link is often impossible in cyber cases. As Mikova writes, “the attribution of cyber-attacks can be a complex process and involve many technical, legal, and political considerations” [7]. However, in cyber cases, it is frequently impossible to prove that causal link. According to Mikova, "the attribution of cyber-attacks can be a complex process and involve many technical, legal, and political considerations" [7]. There are rarely any explicit indications of cyber operations. States may choose not to publicly accuse specific individuals of a crime even in the face of overwhelming evidence in order to prevent political escalation or to protect intelligence sources. On the other hand, public attributions can occasionally be made with weak evidence, which damages credibility. One cannot simply invoke state responsibility or self-defense without clear legal attribution. The law only recognises a state's right to respond to a hostile cyber act if it can link it to another state. Due to this practical gap, many damaging cyberattacks remain unpunished by international law.

4.2. Accountability

Attribution and the issue of consequence are closely related. There is no established system for enforcing international law in cyberspace, even when a state is suspected of doing so. With the exception of war crimes committed through cyberspace under specific conditions, there is no International Criminal Court for cyberattacks. Standard remedies like sanctions, diplomatic protests, or UN actions are slow and politicised. The only options available to victims of cyberattacks are countermeasures or unilateral use of force, as these attacks frequently fall into a grey area that stops short of armed violence. However, countermeasures themselves lack consensus and are subject to legal risks. As a result, accountability in cyberspace is primarily political, involving tit-for-tat espionage or naming and shaming instead of court decisions. According to Mikova's research, states have been using diplomatic responses and public attribution more frequently, but these typically rely on established norms of sovereignty and non-intervention [7]. In summary, international law primarily gives the victim state options like countermeasures and compensation if the act is found to be unlawful; it does not provide a simplified means of holding cyber actors accountable.

4.3. Retrospective Assessment

Cyber operations often unfold over time and have ripple effects that make legal analysis retrospective. Because some of its destructive code was disabled, the Stuxnet attack, for

instance, partially self-corrected over the course of several months [8]. Any legal "snapshot" of the event is complicated by the effects' partial or delayed manifestation. Furthermore, the spread of cyberweapons is unpredictable: The devastation caused by Not Petya spread from Ukraine to every country in the world, impacting private businesses and third states. Although states have historically dominated international law, a cyberattack could injure non-state victims in numerous nations at once. These causal chains need to be untangled through retrospective analysis. For instance, was an allied state whose system got hit by collateral damage part of an armed attack, or just a victim of indiscriminate malware? Regarding transnational collateral harm in a cyber context, there are no explicit legal regulations.

Moreover, cyber operations frequently mix up the terms "force" and "crime". Although malicious software such as WannaCry did not physically destroy infrastructure, it caused significant financial and human costs (e.g., disruptions to NHS hospitals in the UK) [9]. However, unless it is interpreted as a covert armed attack, even extensive economic harm is not specifically protected by Article 2(4). Adams and Reiss point out that although Homeland Security Advisor Bossert and other U.S. officials blamed WannaCry on North Korea, they refrained from referring to it as an armed attack or use of force. This is a reflection of policymakers' apprehension about overstretching definitions in order to trigger legal or military obligations (like NATO's Article 5, which requires all Alliance members to take necessary action to support an attacked Ally in the event of an armed attack). In other words, what an attacker expects their deed to be legally recognised as influences how much care is taken later to label it under the law.

5. Stuxnet: A Case Study in Legal Ambiguity

The landmark instance of a state-sponsored cyberattack that results in physical harm is the Stuxnet operation in 2010. A highly advanced computer worm called Stuxnet invaded Iran's uranium enrichment facility in Natanz, causing centrifuges to spin uncontrollably. Its code targeted industrial control systems and employed a number of zero-day exploits, which went well beyond basic hacking. Although no formal confession was ever made, the majority of the evidence and conjectures point to Israel, with potential assistance from Germany and the United States [8].

From a legal perspective, Stuxnet presents challenging problems. It obviously caused harm, including destroying about a thousand centrifuges and allegedly delaying Iran's nuclear programme by years. According to effect theory, this appears to be a use of force: a foreign actor physically destroyed vital infrastructure. Foltz's analysis specifically states that under the "severity" criterion, Stuxnet "is per se a use of force" because it physically damaged a crucial Iranian interest (the nuclear programme); in fact, if an ordinary bomb had destroyed the same centrifuges, the operation would unquestionably qualify as an armed attack.

Other factors, though, make matters more complicated. The "scope" and human cost, for instance, were relatively restricted. Foltz claimed that Stuxnet "posed no apparent risk of harm to personnel" and that no one was killed. Although strategically significant, its damage was limited. That could indicate that it fell short of the highest thresholds by the standards of some states. According to target theory, Stuxnet could be classified as a use of force because the Natanz plant was arguably a military target (nuclear facilities have dual-use nature). Critics may note, though, that the worm only impacted the electronics of the centrifuges and no other military systems. It might be interpreted as a strike against Iran's scientific programme rather than its military.

Immediacy and timing are also important. The devastating effects on each infected centrifuge took weeks to materialise, and Stuxnet developed over months in at least three phases. Iran had plenty of time to notice the irregularity and react. Legally speaking, this was by no means an

unexpected surprise attack. Foltz comes to the conclusion that Stuxnet would most likely not be considered a use of force by "immediacy," though he believes that immediacy is less significant in light of the obvious physical harm. Additional factors include the operation's direct causal relationship to the damage and its "highly invasive" nature (crossing borders and penetrating air-gapped systems). Despite the unique technical pretext, Stuxnet ultimately possessed all the characteristics of a standard bombardment, with the exception of explosion and manpower.

The main question is: did Stuxnet violate international law? If one applies the effect theory strictly, it seems to have been a prohibited act of force (as Waxman suggests might now be the inclination). However, no authority has formally declared it illegal, largely because attribution remained secret and Iran did not retaliate militarily. According to Article 2(4), using force without a valid reason for self-defence is prohibited. Without a doubt, Stuxnet was not in clear self-defence and lacked a UN mandate. However, states like the US have not been forced to defend it because it was limited and covert. The Tallinn Manual also notes that states often prefer ambiguity in order not to collapse distinctions between lawfulness and state practice.

If the Stuxnet case is to be framed under each theory, then as a tool, it was in essence the "missile" of cyberspace; as an attack on a target, the centrifuges were vital to Iran's nuclear programme, which is an integral part of its state development; and in effect, it caused kinetic damage in the real world. Stuxnet would probably rank highly on the scale-of-force chart according to the Tallinn Manual's list of factors. However, some legal professionals have noted that its scope was modest and distinct because no one was killed and no national capital or city was destroyed. The operation serves as a reminder of how the law is interpreted: it was most likely illegal, but it slipped into an uncertain legal landscape that no treaty specifically addresses. Instead of encouraging warlike language, states are now forced to soften their language in the wake of Stuxnet, referring to it as "espionage," "sabotage," or simply "silent" regarding its legal status.

What can a victim do practically? Iran had the right to complain to the UN or demand compensation because analysts concur that it was likely a state organ operation. Instead of taking legal action, Iran in fact took revenge with its own espionage, the 2012 Flame virus. In cyber incidents, this is very common. Apart from naming the offender, victims hardly ever pursue formal legal options such as litigation and UN action. Iran publicly voiced its outrage in 2010, but did not file a formal complaint. Since no tribunal has rendered a decision on Stuxnet's legality and because international law offers few specific procedures for unauthorised covert attacks, the issue is still unclear. Thus, Stuxnet exemplifies the argument by taking advantage of the legal framework's ambiguity and proving that the law is "not sufficiently defined" for this new domain.

6. Conclusion

In conclusion, the ambiguities of international law have been exposed by cyberwarfare. Theoretically, cyber actions are covered by the UN Charter and current principles: an operation that causes harm to people or destroys property can be regarded as any other military attack. However, because cyber means can conceal themselves behind civilian facades and because the effects are more difficult to measure, states and academics disagree on when exactly the line is crossed. Although the Tallinn Manual acknowledges that any cyberattack that escalates to the level of armed conflict "rises to the level of a use of force," it also demonstrates that states are at disagreements over how to quantify it.

Practically speaking, as Mikova's research highlights, obstacles such as attribution make accountability “difficult.” Even if a law is in place, catch-all legal categories like “use of force” require proof of state accountability, which is frequently absent or secret. Additionally, even

when harm occurs, the victim state can typically only respond in limited ways such as diplomacy, legal countermeasures, or covert action. As Adams and Reiss suggest, governments may prefer "name and shame" strategies over legalistic labelling.

We are thus faced with a paradox: although cyber weapons are real and powerful, the legislation governing them is still in its early stages. Stability is weakened by states' incentives to maintain ambiguity (to permit freedom of action). The paper's analysis of Stuxnet demonstrates how a single, dramatic operation can spark unresolved debate. Clearer international consensus on at least minimal thresholds is most likely necessary for the future. Multilateral norms prohibiting attacks on critical infrastructure, treaty-making on cyber operations, or clarification by organisations such as the International Law Commission constitute some of the suggested actions. Measures that improve confidence and increase transparency (such as states revealing their cyber regulations) may be helpful in the short term. However, the law as it stands now is not sufficiently defined to address the particulars of cyberwar. Future cyber conflicts might continue to take place in legal grey areas in the absence of more precise regulations or accepted practices, increasing risk and uncertainty.

References

[1] Waxman, Matthew. "Cyber Attacks as 'Force' under UN Charter Article 2(4)." Int'l L. Stud., vol. 87, Jan. 2011, p. 44, scholarship.law.columbia.edu/faculty_scholarship/847. Accessed 10 June 2024.

[2] Moynihan, Harriet. "The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention." Chatham House, Dec. 2019, p. 3, www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf. Accessed 24 May 2025.

[3] Schmitt, Michael N., editor. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.

[4] Egan, Brian. "International Law and Stability in Cyberspace." Berkeley Journal of International Law, vol. 35, no. 1, Nov. 2016, p. 175, www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf. Accessed 26 May 2025.

[5] Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law, vol. 48, 2017, p. 738, www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf. Accessed 26 May 2025.

[6] Schmitt, Michael N. "Terminological Precision and International Cyber Law." Lieber Institute West Point, 29 July 2021, lieber.westpoint.edu/terminological-precision-international-cyber-law/. Accessed 24 May 2025.

[7] Achten, Nele, et al. Accountability in Cybersecurity. Edited by Franziska Klopfer, DCAF - Geneva Centre for Security Sector Governance, 2024, pp. 44–69, www.dcaf.ch/sites/default/files/publications/documents/accountability-cybersecurity.pdf. Accessed 27 May 2025.

[8] Foltz, Andrew C. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate." Joint Force Quarterly, no. 67, Oct. 2012, p. 44, ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf. National Defense University Press. Accessed 27 May 2025.

[9] Adams, Michael, and Megan Reiss. "How Should International Law Treat Cyberattacks like WannaCry?" Lawfare, The Lawfare Institute, 22 Dec. 2017, www.lawfaremedia.org/article/how-should-international-law-treat-cyberattacks-wannacry. Accessed 27 May 2025.