(IJPS) 2019, Vol. No. 8, Jul-Dec **e-ISSN: 2455-6270; p-ISSN: 2455-7455**

# EMPLOYABILITY OF CYBER OPERATIONS IN THE FRAMEWORK OF INTERNATIONAL LAW AND INTEGRATION OF THE LAWS OF COLLECTIVE SECURITY, USE OF FORCE, SELF DEFENCE AND ARMED CONFLICT

**Yashika Nagpal**

*Amity Law School, Delhi (Affiliated to Guru Gobind Singh Indraprastha University)*

## ABSTRACT

*As a result of recent cyber-attacks, this article analyses how current laws of armed conflict might be used or changed to meet the new threats. An explanation of cyber assaults is followed by a look at cyber exploitation and cyber espionage as well as how they vary. According to the article, the current corpus of law regulates cyber-attacks such as the UN Charter, IHL, international treaties, and state laws. Existing law only tackles a tiny percentage of possible cyber-attacks, according to the study's findings. There are just a few cases in which a cyber attack may be equated to an armed conflict, and IHL provides a helpful foundation for them. A new international legal framework is needed to address the difficulties posed by cyber-attacks, according to the article's conclusion, because they are global in character.*

***Keywords:*** *Cyber, Operations, International Law, Force, Collective Security, Self-Defense, and Armed Conflict etc.*

## INTRODUCTION

For civilian and military objectives, most countries, particularly the industrialized ones, are becoming increasingly reliant on information and information technology. Having access to cheap, remote, and effective weapons opens the door for adversaries to launch attacks with minimal risk [1]. This means that governments and non-state entities are using internet more frequently to wage war. Combatants can engage in cyber warfare from vast distances, raising ethical and moral questions akin to those posed by those who use drones [2]. Cyber-assailants operate in a completely different environment than traditional terrorists. Cyber-attackers run the danger of being emotionally disconnected from the results of their strikes due to their distance from the horrors of war, raising the likelihood of unwarranted injury, suffering, and collateral damage.

Cyber warfare's legality is still up for debate. Historical interpretations of "armed conflict" by the International Humanitarian Law (IHL) place conventional military weaponry in the light of IHL's requirement for proportionate and required responses. International instruments like as the IHL must be updated to address new threats posed by contemporary technology, such

as cyber warfare. Cyber warfare is now operational, notwithstanding disagreements about how the International Humanitarian Law should be applied to such assaults [3].

## Defining Cyber Warfare

Because an assault might have a wide variety of intended outcomes, the word "cyber war" does not adequately describe all hostile acts in cyberspace. As a result, distinguishing between two types of hostile acts against a computer system or network will be beneficial. Malicious use of computers and the Internet. Destructive cyber attacks are common. The deletion of a computer's hard drive by a virus is an example of a hostile action [4]. It's a "cyber-attack" when an enemy computer system or network (or the information or programmes residing in or transmitting these systems or networks) is attacked using intentional actions and operations that may last for a long time.

## Cyber Operations as a “Use of Force”

"Shall refrain in their international dealings from the threat of force against the territorial integrity or political independence of any state, or in any other way inconsistent with United Nations purposes," reads Article 2(4) of the United Nations Charter. Article 2(4) was revolutionary because it extended the ban to threats even though it made reference to territorial integrity and political independence. It is now commonly recognized that the prohibition extends to any use of force not otherwise permitted by the Charter's provisions. Of course, only threats of force that isn’t already against the law count. 10 If a country engages in illegal cross-border activities, threatening damaging defensive cyber strikes against that country's military infrastructure is not a violation of the norm. Terroristic cyber activities against vital infrastructure in another country are more likely to get that nation to give up its territory than other means. Any transmission of a threat, whether explicit or implicit, is prohibited because it has a coercive impact. Not even threats to the security of the target state, which are not communicative in character, are included in its scope. Accordingly, the introduction of cyber-vulnerabilities that can later be activated destructively into a State's systems does not constitute an actual threat of force unless those vulnerabilities are known to be present and are used by the originating State for coercive purposes against the target State. Most people agree that international customary law prohibits the threat or use of force. Thus, it binds all countries, regardless of their membership in the UN system. Customary law is defined as "general practice recognized as law" under Article 38 of the Statute of the International Court of Justice. State practice and public opinion must coexist, as well as a belief that the activity is carried out or abstained from in compliance with legal obligations [5].

## Uses of Force

Do cyber activities fall under the definition of "use of force" for the purposes of the prohibition? Because the drafters of the Charter adopted a cognitive short cut by defining the

prohibition of the treaty in terms of force as a coercive weapon, there is an interpretative difficulty. As a result, economic and political coercion was permissible, but military force was not, unless there was a specific exemption in the Charter. However, States care less about the tool used and more about the results that result from it. The instrument-based approach made sense when the Charter was adopted since before the emergence of cyber activities, States wanted to avoid the repercussions generally corresponded with instrument-based categories. Although cyber operations are "non-forceful" (that is, non-kinetic), their repercussions might range from mild irritation to death, they do not fit well into this paradigm. There is therefore no international consensus on a clear definition of a use of force in or out of cyberspace, as the Commander of the United States Cyber Command stated during his confirmation hearings [5, 6]. As a result, various countries may have different definitions and thresholds for when force is used. It goes without saying that the word "use of force" includes the use of armed force by a government, particularly military force. As a result, an armed force comprises kinetic forces such as bombs and artillery. No less ridiculous than excluding other destructive non-kinetic acts like biological or radioactive warfare would be the idea that cyber operations that have repercussions similar to those generated by kinetic force are exempt from the prohibition. As a result, cyber activities that cause physical injury to people or tangible items are considered "uses of force" since they are equivalent to using military force. Individuals and property are obviously at risk when an attack is made on an air traffic control system or a water treatment plant. However, as the instance of Estonia shows, most cyber operations are carried out without inflicting any harm. Are such activities, however, prohibited by the ban on the use of force? States will attempt to strike a balance between these opposing goals by taking into account various elements [7], such as those listed below. As a whole, this strategy has held up well throughout time.

- Severity
- Immediacy
- Directness
- Invasiveness
- Measurability
- Presumptive legitimacy
- Responsibility

## Self-Defence

The right of states to use force in self-defense is the second exemption to the ban on the use of force. Article 51 of the UN Charter codifies this customary international law right. To wit: Nothing in the present Charter shall impede an individual or collective right of self-defense if an armed assault occurs against one of the United Nations' members, until the Security Council has taken the necessary steps to ensure international peace and security. While Articles 41 and 42 give some level of protection from assault, their provisions are dependent on the Security Council's execution of them. This item is the sine qua non of the Charter. As a backup plan in case the collective security mechanism fails (or is found to be inadequately

timely), Article 51 offers a method of defense that does not require the agreement of the Security Council. The right to self-defense has consistently shown to be the most effective tool for ensuring national security [8]. In the framework of Article 2(4) and customary law, all armed attacks are "uses of force," with their legality being decided by reference to those standards. Therefore, the right to self-defense only affects the remedies accessible to the victim of an armed attack. Instead, the question in self-defense is whether a violent defensive reaction that would otherwise be an illegal use of force by a State is legitimate (including its form, intensity, length, and extent). As a result, passive cyber defenses, such as those that simply stop assaults, are unaffected; all such defenses are legal. When a group or state launches an assault, the law of self-defense kicks in by inflicting immediate physical costs on the organization or state that launched the attack.

## Armed Attack

Article 51 uses the phrase "armed attack" as its core language and as the cornerstone for the customary law right to self-defense. Even if a cyber operation against a state is equivalent to the unlawful use of force, States do not have the authority to retaliate violently without an armed strike. Creating this contradiction consciously aligns with the Charter's overall presumption against the use of force [9], particularly unilateral action, There is a difference between what the International Criminal Court (ICJ) defined as an armed attack in the Nicaragua case and what it defined as "actions which do not constitute an armed attack but may still entail the use of force." Remember that the Court expressly excluded the provision of rebels with weapons and logistical assistance from the scope of armed attack, but emphasized that such activities might constitute the use of force. Recall. All armed assaults utilize force in some way, but not all forces are armed attacks in the same way. In the absence of an armed attack, redress is restricted to legal non-forceful acts, countermeasures, or going to the Security Council. Practically speaking, this implies that until the use of force escalates to the level of an armed attack, a State exposed to a use of force cannot retaliate in like. Due to the difficulty of tracing a cyber operation's origins, a two-tiered security system is especially useful in the cyber domain. However, it's critical to stress that after an armed attack has been confirmed, no Security Council permission is required before defensive activities, including damaging cyber operations, can be launched.

## Anticipatory Self-Defence

Article 51 exclusively handles armed attacks from a textual perspective. The fact remains that a State does not have to stand by while the enemy prepares to strike; rather, a State can defend itself if an assault is deemed "imminent." After the infamous Caroline incident, Secretary of State Daniel Webster established the commonly recognized concept of immanency. The right to self-defense only applies when "the necessity of that self-defense is urgent, overpowering, and leaving no pause for thought," Webster wrote to his British counterpart during the Mackenzie Rebellion regarding a British entry into American territory to combat Canadian rebels. But even though this occurrence had nothing to do with steps

done in advance of attack (the attacks were already underway) [8, 9], Webster's formula has endured as the standard statement of time thresholds for anticipatory defensive acts; in fact, the Nuremberg Tribunal approved of this instance.

## Criteria for Engaging in Self-Defense

Two legal requirements must be met for self-defense actions: necessity and proportionality. Both necessity and proportionality are legal requirements for a defense, according to the ICJ Both were accepted by the ICJ in the Nicaragua case and later confirmed in the Oil Platforms decision. 74 Necessity dictates that the only alternative other than using force to stop an impending attack or defeat an ongoing one is to use force itself. No one says that the only way to deal with a threat is to use force. It only demands a strong reaction, which may involve diplomatic efforts, economic sanctions, or even law enforcement measures as part of a broader strategy. Instead, proportionality focuses on the question of how much force can be used once it has been determined to be required. Limiting the defensive reaction to to that which is necessary to neutralize a potential assault or repel an ongoing one is the criterion. It does not limit the use of force to that which was utilized in the armed attack since greater force may be required to properly execute a defense or less force may be sufficient. Furthermore, the defensive force does not have to be the same as the armed attack force. It is possible for kinetic actions to respond to cyber activities, and vice versa. Rather than the nature of the armed attack [10], the focal point is the necessity to properly defend oneself against it.

## Evidentiary

The Issues difficulty of identifying an "attacker" is made even more difficult in the cyber world. For example, the attack's origin can be "spoofed". Alternatively, an IP address or other machine-detectable data may be the only trace of a cyber attack's origin or author. Even more time is compressed by the rapidity with which cyber activities are carried out. Before retaliating in self-defense, how certain must the target state is on its attacker's identity? The United States' notification to the Security Council that it had launched its October 2001 attacks against the Taliban and Al Qaeda in Afghanistan was a potentially useful formula, despite the fact that international law does not set a specific evidentiary standard for drawing conclusions as to the originator of an armed attack. Ambassador Negroponte said that "my Government has acquired clear and convincing intelligence indicating the Al-Qaeda group, which is sponsored by the Taliban regime in Afghanistan, played a major role in the attacks." NATO Secretary-General Lord Robertson used the same phrase when he said that the North Atlantic Treaty's collective defense clauses applied to the 9/11 attacks.

## Collective Responses

Countermeasures are taken individually, but defensive actions might be taken together. Article 51 refers to "individual or collective self-defense" and makes this potential clear.

States that have all been attacked can mount a collective self-defense, or a state (or states) that have not been attacked but come to the aid of another state can mount a collective self-defense. Although the fundamental rule is unambiguous in principle, putting it into practice can be difficult. A cyber assault or information that terrorists are preparing a strike might raise questions about whether the collective defense procedures of Article V (the North Atlantic Treaty implementation of Article 51) would be activated. Armed attack alone allows for collective defense [11]; the Security Council is not required to authorize it. However, exercising such right is constrained by the law. ICJ said that only victim-States can decide if an armed assault has taken place and must request help before others intervene on their behalf in the Nicaragua case 81 Absent such, collective activities would be illegal uses of force or possibly armed attacks depending on the nature of the actions (paradoxically, against the State launching the initial armed attack). These conditions are put in place to keep countries from using collective self-defense as a pretext for attacking other countries. This is a reasonable restriction, given the difficulty in tracing the source of a cyber activity. There are notable critics that question the rigorous implementation of these standards, so be aware of that. When collective defense measures occur beyond the victim state's borders, other states may have the right to respond based on their own security interests, according to this theory. The right is allegedly derived from the state launching the armed assault breaching its responsibility to refrain from armed attack. Last but not least, cyber armed assaults may quickly spread across networks and harm States other than those that are the primary target, making this scenario extremely relevant in cyberspace. However, the general consensus is that before a right to collective self-defense can develop, the victim-State must make a request.

## State Sponsorship of Attacks by Non-State Actors

States' accountability for non-State actors' use of force has been discussed previously in relation to the question of state sponsorship of cyber operations. As a result of its interaction with those who undertake cyber operations, when does a State breach the ban on the use of force? However, the significance of State support in the context of self-defense is far greater. It questions whether a State that has not participated in cyber operations but has "supported" them may take aggressive defensive steps, including violent ones. This means that an armed attack can be considered as though it was launched by the government when it is attributable to the government. The Nicaragua case served as the commonly acknowledged standard until the terrorist acts of September 11, 2001 [12]. It was ruled by the ICJ that "an armed attack must be understood as including not only actions by regular forces across an international border, but also 'the sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts if armed force against another state of such gravity as to amount.

## Armed Attacks by Non-State Actors

A growing number of people, such as the anti-Estonian "hacktivists," are turning to cyber operations as a method of waging war against the country's sovereignty. There's good reason to be concerned. There have been discoveries of hacking tools on computers linked to Al Qaeda, and these groups' members are becoming increasingly computer proficient. A captured Al Qaeda computer formerly held dam models and the computer tools needed to evaluate them, making it a valuable target for cyber attacks. Article 51 and the customary law of self-defense have historically been interpreted by international lawyers as only being applicable to armed attacks carried out by one State against another, even though this is not widely accepted. Non-State actors' violent acts came within the criminal law framework. Although Al Qaeda was responsible for the September 11 attacks, the world community viewed them as acts of self-defense and responded accordingly. Numerous decisions of the UN Security Council recognized the right to self-defense as being applicable. Many countries, including NATO and the United States, adopted the same strategy.

## Armed Conflict

While "armed conflict" and "violence" are both considered jus in bello, they are distinct from "violence" and "threat to peace," as well as "act of aggression." According to international law, a State has broken international law when it resorts to force, and a normative flow plan is established for reacting to such violations individually or collectively. Under the jus in bello, on the other hand, IHL is only applicable if there is a "armed conflict." International law, including the four 1949 Geneva Conventions and the two 1977 Protocols Additional (Protocol I for international armed conflict and Protocol II for non-international armed conflict), establishes this rule. To determine whether IHL rules like distinction (the requirement to distinguish between combatants and civilians, as well as between military objectives and civilian objects) or proportionality (the prohibition on attacks expected to cause harm to civilians and civilian objects that are excessive relative to the military advantage anticipated to accrue from the attack) apply to cyber.

## International Armed Conflict

Geneva Conventions, in its common article 2, stipulate that they apply to all instances of declared war or any other armed confrontation between two or more of the High Contracting Parties that may arise. We now have to ask ourselves: What really was the source of the dispute in the first place? Regardless matter whether one party claims that there is no state of war, every dispute between two states that leads to the intervention of military troops constitutes an armed conflict under Article 2, according to an official Red Cross opinion. It doesn't matter how long the war lasts, how much blood is shed, or how many people are involved." Similarly, the International Criminal Tribunal for the former Yugoslavia has said that "an armed conflict arises anytime States resort to force." It's critical to tell the difference between jus in bello "armed combat" and jus ad bellum "armed attacks" since, as previously

said, some scholars argue that minor events don't constitute to armed attacks under the latter doctrine. Moreover, small armed events did not always mark the beginning of a war between States under the conventional definition of the legal notion of "war." Nevertheless, a "international armed conflict" persists so long as the armed forces of two States engage in armed combat. An autonomous group or a person would not qualify as non-State actors acting under State authority. There is no requirement for hostilities to exist. By Article 2, the agreements apply even if there is no violent opposition to "partial or entire occupation..." Detention of people protected by IHL [13], such as fighters, is regarded as an act of armed conflict by the troops of a single State. It makes little difference whether or not the warring parties believe they are "at war."

## Non-International Armed Conflict

Even more difficult is figuring out when a non-international armed war has erupted. Customary international law, Common Article 3 of the Geneva Conventions, and Additional Protocol II, which applies to States parties, include the applicable IHL (AP II). IHL customary rules may or may not apply in international or non-international armed conflicts, but it is undoubtedly a less complete and less thorough body of law than that which governs international or non-international wars. Non-international armed confrontations are ones that are "not of an international character [14]," according to Geneva Conventions Article 3, which reflects customary international law. Such disputes might be classified according to two different characteristics. To begin, the phrase "each Party to the dispute" appears in Article 3. States and organizations with a certain degree of organization and command structure are generally characterized by the word "Party". Individuals or disorganized crowds committing acts of cyber violence, even if intended against the government, do not constitute as acts of terrorism. It wouldn't be an armed war, hence criminal law and human rights law would apply instead of IHL. This describes the vast bulk of cyber activities carried out against Estonia.

## Fault Lines in the Law

Most readers will find the legal analysis presented above to be unsatisfying. It's easy to see the cracks in the corpus of legislation that governs the use of force since it predates cyber operations. As long as coercive means of international relations, notably military power, and their consequences matched closely, the normative system made sense when a country has wreaked havoc on world peace and harmony, it has done so by employing force against both people and things. To prevent those outcomes (death, injury, destruction, and damage) that were seen as the most disruptive to community stability and the greatest threat to state security, instrument-based normative shorthand (use of force, armed attack, and armed conflict) was utilized [15]. There have been debates over the appropriate use of force in situations other than war or whether small border breaches count as armed attacks, and these debates represent a knowledge that the instrumental approach isn't always calibrated properly. Instrument-based warfare was completely upended when cyber operations were

introduced, as they created the prospect of destabilizing consequences other than kinetic ones. By doing so, they undermined the inherent coherence between the normative language used in law to control the use of force and those outcomes that the law intended to prevent as disruptive. To prevent the consequences that governments were most worried about, the "qualitative" approach of prohibiting some actions based on their effects (such as the use of military force and other destructive weapons vs. non-destructive ones) was no longer sufficient. A non-kinetic, non-destructive method of creating consequences that states cannot tolerate was suddenly available; the qualitative shortcut no longer matched up with the quantitative concerns of governments

## CONCLUSION

As a final note, this essay has looked at the extent to which cyber-attacks fall under the existing framework of armed conflict law regulations. Even if it is incomplete and flawed, the current framework for the Law of Armed Conflict gives some assistance for governments looking to establish the scope of authorized offensive and defensive cyber-attacks. Jus ad bellum and jus in bello. For the most part, cyber-attacks aren't governed by this law. In the vast majority of cases, cyber attacks are neither violent attacks or take place during a time of armed conflict. As a result, the existing law of armed conflict does not apply to them. Cyber-attacks are not, however, uncontrolled. The gaps left by the law of armed conflict are filled by many additional legal frameworks, such as international law on countermeasures, local legislation, and so on.

## REFERENCES

1. Brownlie, I. (2012). International Law and the Use of Force by States (p. 362). Oxford: Oxford University Press.
2. Dinstein, Y. (2002). Computer Network Attacks and Self Defense. In M. N. Schmitt, & B. T. O'Donnell (Eds.), Computer Network Attack and International Law (p. 99). International Law Series, Vol. 76, Newport, RI: Naval War College.
3. Gervais, M. (2012). Cyber-Attacks and the Laws of War. Berkeley Journal of International Law, 30, 525-531.
4. Graham, D. E. (2010). Cyber Threats and the Law of War. Journal of National Security Law and Policy, 4, 89.
5. Green, L. C. (2000). The Contemporary Law of Armed Conflict (2nd ed.). Manchester: Manchester University Press.
6. Hathaway, O. A., & Croot of, R. (2012). The Law of Cyber Attack (p. 850). Faculty Scholarship Series, Paper 3852.
7. Jensen, E. (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Stanford Journal of International Law, 38, 207.
8. Lin, H. (2010). Offensive Cyber Operations and the Use of Force. Journal of National Security Law & Policy, 4, 63.

9. Madubuike-Ekwe, N. J. (2017). The Applicability of the Law of Armed Conflict to Cyber warfare: An Overview of Issues. I BUA L. J., 149.
10. Moore, J. N. (2005). Development of International Law of Conflict Management. In J. N. Moore, & R. F. Turner (Eds.), National Security Law (2nd ed.). Durham, NC: Carolina Academic Press.
11. National Research Council (NRC) (2009). Technology, Policy, Law and Ethics regarding U.S. Acquisition and Use of Cyber attack Capabilities.
12. Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 37, 885-937.
13. Sklerov, M. J. (2009). Solving the Dilemma of State Responses to Cyber-Attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent. Military Law Review, 201, 1-85.
14. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press (2017).
15. Wedgewood, R. (2002). Proportionality, Cyberwar and the Law of War. In M. N. Schmitt, & B. T. O'Donnell (Eds.), Computer Network Attack and International Law (pp. 219, 227-230).
16. Wingfield, T. (2000). The Law of Information Conflict: National Security Law in Cyberspace. Falls Church, VA: Aegis Research Corp.