International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 04-02-2021; Accepted: 22-02-2021; Published: 14-03-2021
www.lawjournals.org
Volume 7; Issue 2; 2021; Page No. 104-107

Cyber conflict and jus in Bello – international humanitarian law on cyber attacks

Devi Vara Prasad Romala
Research Scholar, Dr. BR Ambedkar College of Law Andhra University, Andhra Pradesh, India

Abstract
The purpose of this research paper is to examine the provisions of International Humanitarian Law on cyber operations in the context of International Armed Conflicts. This paper will discuss the legal application of the substantive rules restricting warfare to military conflicts involving cyber operations under the Additional Protocol I of the Geneva Convention. The purpose of this paper is to investigate the degree to which cyber operations that don't constitute an attack are governed by the provisions of Additional Protocol I and whether they are considered to be an attack.
In this research paper, the definition for an attack should be interpreted strictly as referring only to cyber operations which lead to death and injury, to individuals or the harm or destruction of artefacts, while international humanitarian law applies to cyber warfare. The implications of this consequence-based interpretation of an 'attack' concept are that most significant safeguards protecting civilians and their artefacts do not apply to cyber operations under Additional Protocol I of the Geneva Convention.
This research paper is limited to only Jus in Bello and does not discuss the Jus ad Bellum or the actions of individuals (e.g., groups of hackers). The technological aspects of cyber warfare will be discussed, as required. This paper deals with identifying cyber operations as attacks in international armed disputes and excludes issues like conflict attribution and classification.

Keywords: cyber warfare, international humanitarian law, Jus in Bello, cyber attacks

Introduction
A logical bomb was pitted in Soviet gas pipeline computer systems in 1982, reportedly triggering a major explosion in Siberia. One of the first known offensive or offensive cyber-attacks is considered. One of the defining features of the digital era is the use and dependency of networked information and communication technologies. In today's industrialised world, computer systems are widely used by governments to operate their vital infrastructure. Increasing relations between computer systems and the physical world have a genuine impact on cyber-attacks. The General Assembly of the United Nations (UNGA) says cyber technology 'can be used for purposes inconsistent with international peace and security goals.'
There is no specific law governing the conduct of cyber operations in cyber warfare and thus there is no common terminology. This has contributed to uncertainty about how cyber warfare is related to international humanitarian law – the laws of war (Jus in Bello).

What is Cyber Warfare?
For more than a decade, experts have been speculating about possible cyber-attack implications. The scenarios—from a blackout in the control system leading to accidents in aircraft to a false message that causes a nuclear reactor to shut off or a dam to open up anticipate significant financial or physical losses. However, there is no settled concept of cyber-attacks for these incidents, much lower than cyber-warfare. The lack of a common concept has rendered the creation of coordinated policy proposals by experts from various countries and the commitment of governments to co-ordinated action a challenge. The technical effort to identify a 'cyber-attack' represents a crucial first step towards resolving the growing threat of cyber-attacks.

In contexts of armed conflict, the term cyber warfare describes military operations that include cyber-attacks and the tactics used by hackers. This definition covers both 'cyber warfare' and 'non-cyber warfare' within the category (Cyber strategies, methods). Cyber warfare denotes State actors' participation, while other actions like cybercrime or terrorism relate to individuals' illegal or terrorist activities through using cyberspace.

The Relation Between Cyber Warfare and International Humanitarian Law
First, the relationship now a day are interwoven and intertwined between international humanitarian law and cyber-war. The guidelines that military personnel have to obey in engaging in war are, we recognise, the international humanitarian law (IHL). These war laws define what acts against non-combatants, troops and unauthorised combatants may or may not take. One of IHL's main aspects is that in wartime civilians and non-combatants cannot be killed or treated inhumanely. Many weapons, including bulleting, chemical and biologic weapons, laser blinding weapons and anti-personnel mines, are banned by International humanitarian law.
The 21st century is the age of many modern ideas of military warfare. Each of them is the theory of electronic warfare. In the place of traditional weapons, computer networks are used for cyber-attacks, and satellites have far more accurate pictures than human spies or identification units ever deliver. However, since cyber technology is the latest phenomenon of the 21st Century, the IHL is facing the new challenge of adapting moral expectations for cyber warfare. Although apparent wars on land, sea and air can be regarded as questions under current rules and customs of war, cyberspace is undefined. Whereas cyberspace itself is unphysical, it can have a major impact on the physical

environment. Logic bombs and computer viruses can interrupt anything from power grids and financial markets to nuclear and hydropower plants.

Also, it is worth stressing the key issues in humanitarian law as regards the connection between IHL and cyber warfare: Inter-alia. Jus in Bello collectively referred to as war law, armed conflict law (Lo AC) or international humanitarian law (IHL), is the portion of national law that offers immunity to individuals no longer engaged in conflicts that limit fighting means and strategies.

IHL law consists of two sets of treaties: The Hague Conventions and the Geneva Conventions. The Hague Conventions deals with military zones, including city laws from 1899 and 1907, and a lot of other conventions and agreements banning the use of such arms and military strategies. The second Geneva Convention covers the defence of civilians, injured and sick during land and sea, along with the four 1949 Geneva Conventions. Protocol III about the adoption of a distinct logo was added in 2005. International law regulates the connection between different states and individuals. Civilians and medical and religious military personnel are covered under international humanitarian law. International humanitarian law forbids all means and methods of warfare that do not differentiate between combatants and non-combatants or discriminate between civilians and combatants.

Cyber war is described as a hostile act against an enemy intended to locate, kill, disrupt, modify, destroy or move data stored in a computer, or transmitted via a computer network. It is an assault that is embraced by many countries to minimise their frustration and to prevent the actual war situation. China's attacks on Google, cyber war against Ghost net spyware network, and the cyber assault on the Pentagon are examples of cyber warfare. Facebook taught us that we can never be alone, however, it is appropriate when it is not a large company. Some scholars argue it is very difficult to extend the current IHL legal regime to the cyber domain because of the technicality of the subject matter.

Application of International Humanitarian Law to Cyber Warfare

International humanitarian law applies to cases when two or more countries are involved. Regardless of the severity or duration of the struggle and regardless of their initial use of force against each other, commit hostility. An armed conflict needs to occur factually. International humanitarian law aims at governing methods and strategies of fighting by harmonising military and humanitarian needs. There are not only Geneva Conventions I - IV but additionally Protocols I - III that are aligned with the Geneva conventions. The Conventions of Geneva represent all the customary law. It is more contentious the status of the additional protocols because they have not the same degree of recognition

Cyber Space has unique features which have led to it being categorised as a 'fifth field of battle'. The effectiveness of the laws upholding human rights has been a point of contention. International humanitarian law (IHL) applies to all sorts of warfare, meaning nuclear warfare as well. Cyber operations arising in case of armed conflict are regulated by international humanitarian law.

This type of acts can be carried out without physical abuse. If cyber operations are autonomous and they are not sanctioned by a legitimate state authority, they constitute attacks beyond the bounds of legitimate state activity. However, this scenario is considered to be an imperative of an "armed conflict," and is not sufficient for actions of particular nature and severity. The applicability of humanitarian international law for cyber warfare was defined by the UN and reaffirmed by many states. Thus, cyber operations have a higher risk for use in combination with conventional warfare.

The lack of cyber-specific protections in humanitarian international law doesn't mean non-regulated cyber warfare. The Martens Clause does not agree that anything that is not expressly excluded by the relevant treaties is also allowed to ensure that current requirements apply to new circumstances or technologies. In the case of Nuclear Weapons, the ICJ rejected the fact that the humanitarian laws of the IHL "before the invention of nuclear weapons had developed rules and principles," and that "there can be no question about whether humanitarian law applies to nuclear weapons." The same is true for electronic warfare. There is also a legislative provision to review the introduction of new weapons following international humanitarian legislation.

International Response to Violence under Additional Protocol I.

Attacks are described in Article 49(1) of Additional Protocol I as 'acts of violence against an opponent, whether in an offence or a defence.' The Commentary indicates that attacks must require military action since civilians are likely to be harmed by the war in this way. There is an "act of violence" whether it results in death or injury to individuals, or destruction of objects and/or harm to property. This word encompasses all violent acts, whether or not they are non-violent, such as biological or chemical weapons. Passing unfavourable situations or disturbances does not make an act violent. This term is only for conventional military warfare. The meaning of "an attack" differs from other uses of the word "attack," such as a "military attack" under the UN charter.

Cyber Operations as Cyber Attacks

A cyber-attack is 'an offensive or defensive cyber-operation reasonably intended to injure or kill persons or to harm or destroy objects.' Deaths or large-scale property damage may be identified, as is the case with conventional weapons, as an assault under humanitarian law by cyber activity. the essence of the attack is not the deciding factor. An attack under this description is a Cyber operation aimed at a power plant and deprive a hospital of power which leads to patient killing. As with traditional attacks, the impact of harmful or disruptive cyber operations shall be understood through an equation of the physical effects of the action. This description can include cyberattacks that, for example, manipulate water Dam Control Systems, leading to significant downstream damage and possible people's death or injury. Operations that simply crash through firewalls or instal malware on enemy computers cannot be identified as attacks unless they produce the necessary harmful effects. Likely, cyber operations that exclude target data from the attack definition, because data in the context of the Additional Protocol I are not regarded as an entity.

Cyber-operatives that disable the utility of an organisation can count as an attack if the restoration of the utility requires the physical components to be replaced or the system or particular data to be reinstalled. This functionality test was

developed by the Tallinn Manual drafters. The need to replace components is an indicator of injury, which could be contrasted with the physical attack of the same objective. The same is true of the data and an attack is known to be a Cyber activity that kills even a small volume of data vital to the functioning of the computer system.

Principles for cyberattacks

Cyber operations may be configured to deliver a wide variety of results and may not have physical impacts. The key consequences of cyber operations are almost always secondary to the attack itself, which leads one to doubt whether or not the attack took place and whether the attack is incidental to the alleged effects. The complexity of cyber operations led to controversy on the scope of the definition of an attack, as much of the law governing hostilities is organised around attacks and not surgery. Qualifying an act as an attack enables the constraint imposed on attacks under Additional Protocol I. Operations under Additional Protocol, I have the same rules as kinetic attacks Operations under Additional Protocol I have the same rules as kinetic attacks. The applicable law includes the distinction principle, the ban on the attacks on civilians and civilian ~~property, the prohibition of indis~~criminate assaults, the principle of proportionality, the duty to take care when carrying out any military operations and attacks and the necessity to take precautions against the consequences of these attacks.

In legal doctrine, there is a difference between people who accept the broad interpretation of the supplementary protocol I and who aim to protect civilians from any actions connected with hostilities, Defence limited to violent acts (i.e., attacks). Both positions reflect a restrictive approach (which limits the use of cyber operations by law) and a permissive approach (which permits a broader variety of cyber operations).

Interpretation of the Additional Protocol I with Cyber Operations

The Passive Method.

Article 48 of the Additional Protocol I allow the parties to a conflict to provide for the protection of civilians and the prohibition of attacks on civilian objects. The theory is based upon the 1868 St Petersburg Declaration, which states that "in war, the only legitimate objectives that states should strive for are to weaken the military forces of the enemy". It is considered an "elementary principle of customary international law." Which is interpreted by referring to ‘all movements and activities related to wars that are performed by the armed forces.' The ICRC interpreted the scope of the article to include only war operations during which violence is used. Despite its defining military operations generally, the reference is to include attacks. The ICRC adopts this view by specifying that only armed attacks in compliance with the Additional Protocol I are subject to the concept of distinction.

The principle of distinction is observed in military law that restricts civilian harm. Civilians are given the ‘whole of the legislation. 'Under Article 51 of the Additional Protocol I. it has guaranteed fundamental security against the repercussions of hostilities, and not subject to attack. Besides, the attack on homes and public property that is under international law is forbidden. Also, reprisal attacks that target civilians are regarded as unconstitutional. According to Commentary, it is under Article 49(1) of the current Additional Protocol I that civilians and civilian items are not to be the subject of direct attack, but also interpreted the clause only means direct attacks on civilians are unlawful. All civilians are safe from cyber-attacks. However, civilians cannot be targeted.

Article 57(1) of the Additional Protocol I require "constant care" for "sparing civilians, civilian objects" in performing military operations. The word military activity implies any armed forces actions, exercises and other operations. The provision requires that the parties to a conflict be constantly sensitive to the impact on civilian populations and civilian artefacts of their actions and attempt to prevent unnecessary consequences thereon, for example by getting technical experts to decide whether sufficient precautionary steps were taken. The provision requires The ICRC Commentary considers the need to add to the distinction concept to cover the general responsibility to respect civilians. The Tallinn Manual interprets the duty to extend to all sorts of hostilities, covering cyber operations as well as cyber-attacks. The permissive approach also allows for the duty to be treated as another collection of attack criteria as stated in its subsections 57(2) - (5). It is interesting that, according to its title, Article 58 of the supplementary Protocol I apply exclusively to attacks. There can also be no international custom support that Article 58 includes operations as well.

The Conservative Approach

The Conservative approach has been criticised and opposed to several factors. In its final sentence, the Commentary to Article 48 of the Additional Protocol I describes military operations as ‘all activities relevant to military behaviour.' The word "armed conflict" is a wider definition that includes "all military operations associated with war". There is strong reason to insist that war is any military operation. This means that the rules should apply also to non-violent operations that are a part of the hostilities. It is safe to assume that the first sentence of paragraph 49 does not apply to assaults. The Commentaries to Articles 51 and 57 use the word 'combat' for all types of violence.

Another point is the objection from the strict way of handling the ‘strategic individual'. Since it relates to neutralisation, this ruling may be applied to both non-kinetic and kinetic means. Cyber operations only have applicability even in the absence of kinetic consequences. Argumentation herein may be denied, provided that the concept of an attack under Article 49(1) of the Additional Protocol I does not depend on the definition of its target under Article 52. (2). The provision only applies after a crisis has been confirmed to be an attack.

Conclusion

This paper has shown the legality of a 'defence' in the cyber domain. Cyber activities that are not physical are not subject to the moral constraints that are reflected in the Law of War. The case studies demonstrate this because a large-scale yet non-physical cyber-attack may be legitimate while a smaller-scale physical attack that targets a few people is blatantly unlawful. This finding is contrary to the established principles of international humanitarian law. Although compelling points, the use of cyber operations should be strictly limited due to humanitarian concerns. The future state-based experience will dictate how the concepts of an attack will adapt to cyber warfare.

References

1. Harrison Dinniss H. Cyber Warfare and the Laws of War. United Kingdom: Cambridge University Press, 2014.
2. Roscini M. Cyber Operations and the Use of Force in International Law. United Kingdom: OUP Oxford, 2014.
3. Cyber Warfare: A Multidisciplinary Analysis, 2015. United Kingdom: Taylor & Francis, 2015.
4. Research Handbook on International Law and Cyberspace. United Kingdom: Edward Elgar Publishing, Incorporated, 2015.
5. Moir L. The Law of Internal Armed Conflict. United Kingdom: Cambridge University Press, 2002.
6. Knake R, Clarke RA. Cyber War: The Next Threat to National Security and What to Do about It. United States: HarperCollins e-books, 2010.
7. The Oxford Handbook of the Use of Force in International Law. United Kingdom: OUP Oxford, 2015.
8. Delerue F. Cyber Operations and International Law. United Kingdom: Cambridge University Press, 2020.
9. Shackelford SJ. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. United Kingdom: Cambridge University Press, 2020.
10. Chinkin C, Kaldor M. International Law and New Wars. United Kingdom: Cambridge University Press, 2017.
11. Glorioso L. Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative. Germany: Springer International Publishing, 2016.
12. O'Donnell BT. Computer Network Attack and International Law. United States: Naval War College, 2002.
13. New Technologies and the Law in War and Peace. United Kingdom: Cambridge University Press, 2018.
14. Geers K, Czosseck C. The Virtual Battlefield: Perspectives on Cyber Warfare. Netherlands: Ios Press.
15. Gray C. International Law and the Use of Force. United Kingdom: OUP Oxford, 2008.
16. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. (n.d.). Germany: Springer International Publishing.
17. Khan, Asif and Ullah, Maseeh and Rehman, Fazal and Ghani, Abdul, Cyber Attacks in International Law: From Atomic War to Computer War, 2017.
18. Duncan B. Hollis, Why States Need an International Law for Information Operations, 11 LEWIS & CLARK L. REV. 1023, 1042, 2007.
19. Hathaway O, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W*et al*. The Law of Cyber-Attack. *California Law Review*. 2012; 100(4):817-885.
20. Customary International Humanitarian Law. United Kingdom: Cambridge University Press, 2005.
21. Ball D. China's Cyber Warfare Capabilities. Security Challenges. 2011; 7(2):81-103.
22. Diamond E. Law and National Security: Selected Issues (pp. 67-84, Rep.) (Baruch P. & Kurz A., Eds.). Institute for National Security Studies, 2014.
23. Chinkin C, Kaldor M. International Law and New Wars. United Kingdom: Cambridge University Press, 2017.
24. Hathaway O, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W, Spiegel J *et al*. The Law of Cyber-Attack. California Law Review. 2012; 4), 817-885.
25. Zimmerman C. Ten Strategies of a World-Class Cybersecurity Operations Center. (n.p.): MITRE Corporation, 2014.
26. Protection of Civilians. United Kingdom: OUP Oxford, 2016.
27. Liivoja, Rain, Tim McCormack, "Routledge Handbook of the Law of Armed Conflict".
28. Mavropoulou E. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. Journal of Law & Cyber Warfare. 2015; 4(2):23-93.
29. Schmitt, Michael N. Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics (December 4, 2012). Harvard National Security Journal Feature, 2013.