GLSR Global Legal Studies Review

Cite Us

DOI: 10.31703/glsr.2021(VI-II).17 p- ISSN: 2708-2458 e- ISSN: 2708-2466 L- ISSN: 2708-2458

Pages: 137–144 Vol. VI, No. II (Spring 2021) URL: http://dx.doi.org/10.31703/glsr.2021(VI-II).17

The New Frontier of Warfare: Evaluating the Role of International Humanitarian Law in Cyber-Crimes

Saima Razzaq Khah * Rubab † Azmat Ali Shah ‡

Abstract: *People & governments have become dependent on computer networks in the last few decades. Both the military & people use these networks to do things like shop online and control radars. A country's computer network system is very important from a military point of view in war. International Humanitarian Law is hard to follow when computers are used to help the military win a war. Schmidt (2017) there are at least two ways to look at whether or not IHL applies to cyber war. These ways of doing things are "permissive" and "restrictive." After looking at both of these ways of thinking, this article suggests that the most important thing to consider when applying the IHL to cyber-operation during a war is how it affects civilians.*

Key Words: Modern Warfare Techniques, Cyber Attacks, and International Humanitarian Law

Introduction

As long as there have been people, there have been wars. In every area, people have made progress, and war is no different. Over time, it has become more complicated and better. Every part of the war has changed and gotten better over time, including how soldiers are trained, how they fight, the methods and techniques of war, how advanced weapons are, and how wars are fought. When new tools and methods are used in war, the rules and standards that govern it are always changed (Roscini, 2014).

In the international law of conflicts, there are two groups. Each side in a conflict has its own set of rules that cover different parts of a fight. The first set is called jus ad bellum, and it says whether or not an armed conflict is legal in and of itself. In other words, it has to do with the use of force by a state in an armed conflict and says when it can be used, when it can't be used, and when it can be used anyway. The jus in Bello, on the other hand, is about how wars should be fought. It tells how to attack, how to tell the difference between civilians and combatants, and how to tell the difference between civilian objects and military objectives. Jus ad bellum is about states, and it only applies to wars between countries. On the other hand, just in Bello applies to both international and non-international wars (Pictet, 1985).

Since the early 1990s, lawyers have been arguing about how to handle military operations that use computers. People, businesses, and even the government all use them. They are used to keep services and supplies running, manage air traffic control, railways, banks, industries, dams, and nuclear facilities and installations, and keep track of air traffic. Because of this, from a military point of view, a country's computer network system becomes very important during a war.

Most wars happen on land, at sea, or in the air. Because computers and network technologies are getting better and the military is using them more and more, a new battleground called "cyberspace" has come into being. Experts say that it is "a physical and non-physical environment in which computers and electromagnetic spectrum are used to store, change, and exchange data over computer networks." This kind of war is hard to find and can't be seen, but it could have the same bad effects as a regular war with physical weapons. This has caused problems for the laws that govern armed conflicts, whether they are

* Lecturer, Department of Political Science, Gomal University, Dera Ismail Khan, KP, Pakistan.
† Lecturer, Department of Political Science, Gomal University, Dera Ismail Khan, KP, Pakistan.
‡ Assistant professor, Department of Political Science, Gomal University, Dera Ismail Khan, KP, Pakistan.
Email: dr.azmatalishah@gu.edu.pk

Citation: Khah, S. R., Rubab & Shah, A. A. (2021). The New Frontier of Warfare: Evaluating the Role of International Humanitarian Law in Cyber-Crimes. *Global Legal Studies Review, VI*(II), 137-144.
https://doi.org/10.31703/glsr.2021(VI-II).17

based on jus ad bellum or jus in Bello [Bradley, 2020].

This study looks at how hard it is to use IHL for cyber operations that are done to get a military advantage during a war. As the Geneva Conventions of 1949 and the Additional Protocols to them of 1977 were written when wars were fought with "kinetic weapons," they do not cover cyber operations or cyber-attacks. Cyberwarfare, on the other hand, is different from other kinds of fighting, which is why people still talk about it. Cyberwar is not fought on traditional battlefields or in places like the air, the sea, or the land. It happens on the Internet. Its "weapons" are very different from those used in traditional war. When trying to apply IHL to cyber warfare, words like "conflict," "armed attack," "use of force," "military and civilian objects," etc. have different meanings. So, it's more important than ever to explain the IHL and how it applies to the subject at hand [Dörmann, 2018].

Applicability of IHL to Cyber Attacks

A lot of lawyers know about the different kinds of hostilities that can be used to give a military side an advantage in a fight by using a computer network. But they disagree about whether or not the law should cover these kinds of operations. How does the IHL make something illegal in cyberspace? Does the IHL cover all cyber operations that happen during a war? Since International Humanitarian Law (IHL) protects people and civilian property from "attacks," the main point of contention would be what IHL means by the word "attack." So, the same question could be asked in a different way: when does the law consider cyber-operation to be an "attack"?

International Humanitarian Law is based on the idea that there are separate things in the world. People have said that the goal of IHL is to limit the damage that wars do to people, property, infrastructure, and other things that people need to live. When the International Humanitarian Law (IHL) says that cyber operations are the same as "armed attacks," the question becomes very important. People are immediately drawn to the idea of difference, and the IHL is stricter in general [Droege, 2012].

The AP-Articles I's 48-58 have the most information about how to protect civilians during a war. There are many different ideas about how these rules apply to cyber operations. Article 48 of the AP-I says that all sides in a war must always tell the difference between civilians, combatants, civilian objects, and military objectives. It says that "only military goals" should be the focus of the parties' efforts [Schmitt, 2002]. Article 51 of the AP-I says, "The civilian population and individual civilians will be generally protected against dangers deriving from military operations." This section protects everyone who fits the definition of "civilian" in Article 50 of the AP-I from "dangers deriving from military operations." Legal experts have a lot to say about the phrase "dangers from military activities" in general and its last part "military operations" in particular. "Military operations" is a pretty broad and general term, but if it is used in a strict way, it could limit every operation that involves armed forces doing things during a war. At its most limited, this phrase could also mean every "cyber operation, " such as what military forces do during a war. Also, the phrase "from where risks come" needs to be thought about before being used. Danger can mean a simple worry or threat, but it can also mean a lot of deaths and damage [Schmitt, 2012].

In the next paragraphs of the same Article 51 of the AP-I, which tells both sides of a war to protect civilians, the word "attack" is used instead of "military operations." Because of this disagreement, there are two ways to look at how IHL should be used in cyber operations: the liberal approach and the restrictive approach.

The Permissive Approach

Schmitt, who was one of the first people to support this strategy, thinks it's okay because it "allows a wider range of cyber operations against civilians." He says that IHL is in effect as soon as there is a military conflict. What does it mean when there is a conflict? In response to this question, he says, "An armed conflict happens when one group hurts, kills, damages, or destroys another." The phrase also includes actions that were meant to have such results or were expected to have such results. As you'll see, this point of view gives people who like this approach a basic set of rules for figuring out when IHL would apply to cyber operations. His arguments are based on Articles 51 and 52 of the AP-I, which say that people are protected and that "attacks" are not allowed during armed combat. Some people say that article 49 of the AP-I defines "attacks" in the context of IHL as "acts of violence against the enemy, whether in attack or defense." So, the IHL says that only "military operations" that include "acts of violence" can be called "attacks" [Schmitt, 2014].

Using this line of thinking to try to apply IHL to cyber operations, which are usually not "violent" to begin with, is not a good idea. Schmitt says that this dilemma is clear when it comes to normal kinetic operations, but it may not be so clear when

it comes to cyber operations, which are not inherently violent, because both Article 48 and the Commentary talk about the use of violence [International Committee of the Red Cross, 2019]. Even though the principle of differentiation is written in terms of "military operations," it is clear that the standard does not apply to all military activities. To back up his point of view, he says that states at war have never thought of spying, spreading propaganda, or handing out leaflets as "violent." So, he comes to the conclusion that the article in question "covers all violent acts." IHL says that any cyber activity that kills or hurts civilians or damages or destroys their property is an "attack" and is therefore against the law. On the other hand, cyber activities that don't hurt civilians or their property don't meet the definition of an "attack" and aren't covered by the relevant parts of the AP-I [Taddeo, 2018].

The Restrictive Approach

Along with the "permissive" approach, some scholars have a more restrictive view of how International Humanitarian Law (IHL) rules apply to cyber operations. People who support the limited approach think that the kind of military action doesn't change whether or not IHL rules apply. Instead, the people who made the protocols thought about how to protect civilians. They say it doesn't matter if a cyber-operation destroys something or not. Dormann says that it doesn't matter if a cyber operation destroys the thing it was meant to get rid of or not. He talks about Article 52 (2) of the AP-I, which says that attacks can only be made against things that help the military or whose total or partial destruction or neutralization would give the military side of the enemy an advantage. He says that the word "neutralization" in that article makes it sound like it doesn't matter how the target object is turned off for an operation to be considered an attack [Ducheine & Schmitt, 2018].

Droege doesn't like the permissive approach for many different reasons. She thinks that the principle of distinction requires warring parties to tell the difference between civilians, soldiers, and civilian objects. This is because the goal of the principle is to keep people safe. Article 48 of the AP-I, the law in question, says that they can only use their activities for military goals. So, Article 3 of the IHL says that any operation that is aimed at or directed at a civilian person or object is illegal. Schmitt's claim that some military activities, like propaganda or other psychological operations, may be aimed at civilians is based on a misunderstanding of what "military operations" are (Schmidt, et al., 2013). In contrast to the permissive approach, she says that attacks must be limited to physical means of war because they are always acts of violence. An attack could also be a military move that doesn't start out violently but ends up that way. She gives the example of weapons that use chemicals and germs. Even though there is no physical force involved in using these weapons, the results are horrible, so it is considered an attack. In other words, a military operation is an attack because it leads to violence, not because it uses violence. She also says that Schmitt missed the fact that "neutralization" was meant to include attacks that stop the opponent from using something without destroying it. For example, cyber interference with an enemy's air defense computer system that makes it useless for a while would be considered "neutralization" and an "attack" under IHL, even if no physical infrastructure was damaged [Rosenzweig, 2018].

Critical Analysis of the Permissive and Restrictive Approaches

The goal of international humanitarian law is to find a middle ground between the needs of the military and the need to protect civilians during war. So, the whole point of IHL is to protect civilians and their property. In order to keep this balance, the IHL has a rule called "distinction" that both sides of a conflict must always follow. Article 48 of the AP-I sets up the principle of distinction and says that people who take part in a war must: "focus solely on military goals." In this article, the word "operations" is used in a broad sense to mean everything that fighting parties do to gain a military advantage. As was already said, people who believe in the permissive approach say that the following articles use "attacks" instead of "operations." This means that only cyberattacks are covered by IHL. They use what the AP-I says in Article 49 as an "attack" [O'Connell, 2017].

Article 48 is based on the idea of "distinction," and it protects civilians and civilian property during a war. This protection is not only wide but also always there because the combatants are always expected to tell the difference between military and civilian goals. The main goal of IHL is to protect civilians from all kinds of military actions that are meant to hurt them. When cyber operations are used in a war, both sides must always keep in mind the concept of distinction.

In response to the difference between "operations" in Article 48 and "attacks" in some of the following articles, this author has pointed out that the parts of the treaty that use the word "attacks" forbid the warring parties from doing

certain things. According to the definition of "attack," these are violent acts done to gain a military advantage over the enemy, which is a military objective. These rules say that the side that is attacking can't change how well civilians are protected during an attack. This is because the IHL doesn't ban armed conflict in and of itself, and both sides are allowed to get a military advantage over the other. Still, it does control how wars are fought, which limits the rights of both sides. In other words, the word "attacks" has been replaced with "operations" to describe the steps that protect civilians by setting up the differentiation principle. "Operations" is also a more general and broad term than "attacks."

On the other hand, the warring sides have been called an "attack," which limits their right to fight. "Attack" is a military term for a specific, targeted act of violence done to gain a military advantage [(Corn & Jensen, 2011)].

Think about the idea that killing, hurting, damaging, or destroying something is always part of an "act of violence." In response to this idea, Droege and Dormann said that the word "neutralization" in article 52 (2) doesn't always mean that an object is fully or partially damaged or destroyed. They say that an object has been "neutralized" if the enemy can't use it to get a military advantage, either temporarily or permanently. Even if the thing wasn't broken, this is still true. Neutralizing a computer system is what happens when a cyber operation is used to attack it in a way that slows it down or stops it from doing something. Schmitt, M. N.& Billingsley, L. [(2014)]. What makes something an "attack" or not depends on how it affects civilians and what happens because of it. Not every time the same operation hurts or kills a person or damages or destroys a civilian object is it the same operation. If we take the permissive approach supporters' point of view, as Droege put it, "this would lead to the conclusion that bombing a single house would be an attack, but cutting the power to thousands or millions of people would not be."The IHL protects both civilians and property that belongs to civilians. Due to the word "object," experts disagree on whether data saved on a computer or hard disc can be considered an "object" or not. And if cyberspace is used to attack computer data, would this be an "attack on a civilian object" under Article 52 of the AP I?

The term "object" is not defined in the API, but supporters of the permissive approach say it means something that can be seen and touched. Under international humanitarian law, "data" is not considered an "object" because it is none of these things. Some experts don't agree with those who say the permissive strategy is best. Article 48 of the AP I says that all military actions can't hurt civilians or civilian property. They say that if the first opinion is accepted, the law would be limited, and civilian datasets and information could be put in danger, no matter how important or valuable they are. A position like this would also go against the law's main idea, which is that people and civilian property should always be protected.

As this study points out, Article 51 (2) limits military goals to "those items which, by their nature, position, purpose, or use, make an effective contribution to military action." It also says that if the complete or partial destruction, seizure, or neutralization of a military target could give the military an advantage in a given situation, it must be done. The words "nature, location, function, or use" are very important to this article. Since computer data is different from other things in its "nature," it can only be "useful and purposeful" if it is "placed" in the right place, like on a disc or other storage device. If a resident's data that is only used for civilian purposes is attacked during a war in a way that makes it useless, like by deleting it from its storage location or making it wrong, and this makes life harder for civilians by, for example, disrupting their power or air traffic control, it would be a violation of API's promise to protect civilians in general. When both of these ways of thinking are carefully looked at in light of the principles of differentiation, it seems that what makes an act an "attack" under IHL is not how violently it is done, but how violently it affects or is likely to affect civilians. If and when these things happen because of a cyber weapon of war, it would be right for the International Humanitarian Law to apply the rules that apply.

Conclusion

When people get better at something, they have to change the rules, whether they are social or legal. The world is changing, and so should the laws. Many people want to know how the IHL works with the new ways, methods, and techniques of war. In the past few decades, the field of computer network systems has grown by leaps and bounds, and more and more civilian and military installations and infrastructure depend on them. Using cyber tools during a war to get a military edge over the other side has caused a debate about how the rules of war work. Bad things could happen if they are used against people or things that belong to the public. Even though some experts think that the current legal

system doesn't keep up with changes in cyber technology and that a new convention is needed to answer questions that come up during a cyberattack. Some people might think that these ideas are closer to the "ideal," but putting them into action is a long process that could take years or even decades. As fast as computer technology changes, so do the problems that come with it. During wars, cyberattacks could happen to anyone in the world, which could be dangerous. This is one reason why a lot of experts and groups are talking about the issue and trying to figure out the best way to use the laws that are already in place. International law is also strong and flexible enough that, if it is interpreted correctly, it can be used in new situations. Most experts agree that international law is strong enough and changes quickly enough to be used against them. But they each have their own ideas about how it should work. People have talked about the problem for more than a decade and have come up with two ways to deal with it: the permissive and the restrictive. The first one gives cyber operations against civilians during a war more freedom, while the second one limits them. Experts don't always agree on when a cyber operation can be considered an "attack" under International Humanitarian Law (IHL) and be governed by its rules. Each side of this debate has come up with a different way to look at the problem. Each has good and bad points that help them make their case. During the current debate, the focus should stay on the core principles of the IHL, like the principles of distinction, precaution, proportionality, etc., and they should be applied the same way to all kinds of hostilities during an armed conflict, no matter how they started.

Recommendations

Cyberwarfare is getting better, so it is thought that it doesn't have enough resources. There isn't much evidence that the way states deal with the issue has changed. Still, scholars have different ideas about how the ideas and rules of IHL should be used in cyber warfare. It is important to remember that the goal of IHL is to protect people who are not taking part in the fighting during a war. So, whether or not IHL applies to cyberattacks, the goal should be to protect them from the effects of war, whether or not IHL applies. Second, the military network should be kept as far away from the civilian network as possible. At the moment, both systems use the same system. The same computer network is used by both civilian and military organizations, which makes it hard to tell them apart.

Cyberattacks may meet the criteria for "use of force" (Article 2 of the UN Charter), "armed attack" (Article 51 of the UN Charter), and "attack" (in the sense of AP I) in certain situations, according to a detailed look at the issue in this thesis. In order to apply IHL to a cyberattack, it is recommended that the impact and results of such an operation be put first. When a hack has effects in the "outer world," it's a big deal, and if those effects hurt civilians, it goes against Art. 48 of AP I. It doesn't matter much if cyberattacks were done violently or not. What matters is how these attacks hurt civilians. It is against the law to use the internet to hurt civilians or civilian property. If a cyberattack during a war is likely to hurt people a lot, it should also be banned. During a war, a cyberattack can only be used to hit a military target, not civilians, to give one side an advantage over the other. Also, all of the rules of International Humanitarian Law (IHL) work the same way when it comes to a cyber-attack. Civilians should be protected from cyberattacks the same way they are from other kinds of war. IHL says that it is against the law to use cyberspace to hurt civilians. The concept of proportionality should also be used for cyberattacks. The party doing the attack should decide how much of a military advantage it wants and how likely it is that these attacks will cause other damage. At this point, it seems hard to answer every question about whether or not IHL applies to cyber warfare. But if we recognize that time-tested principles of IHL are flexible, if we hope that state practices regarding the use of cyber means and methods of warfare will change over time, and if we have a deliberate, healthy, and objective debate about the legal and technical issues involved, we can hope that we will feel more comfortable applying laws to cyber warfare in the future.

References

Bradley, M. (2020). From armed conflict to urban violence: transformations in the International Committee of the Red Cross, international humanitarianism, and the laws of war. *European Journal of International Relations*, *26*(4), 1061-1083. https://doi.org/10.1177/1354066120908637

Corn, G. J., & Jensen, E. (2011). Cyber-attacks and the law of war. *International Law Studies, 87*, 97-130. https://lawcat.berkeley.edu/record/1125035/files/fulltext.pdf

Dörmann, K. (2018, September 16). *Applicability of the Additional Protocols to Computer Network Attacks*. International Committee of the Red Cross. https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf

Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533-578. https://doi.org/10.1017/s1816383113000246

Ducheine, P., & Schmitt, M. N. (2018). International law and cyber operations: What is the applicable law? *Journal of Conflict & Security Law, 23*(2), 267-293.

ICRC (International Committee of the Red Cross). (2019). *International humanitarian law and cyber operations during armed conflicts*. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

O'Connell, M. E. (2017). The international law of cyberspace: Moving beyond the Chicago school? *Virginia Journal of International Law, 57*, 117-175.

Pictet, J., & Rights, I. I. O. H. (1985). *Development and principles of international humanitarian law: Course Given in July 1982 at the University of Strasbourg as Part of the Courses Organized by the International Institute of Human Rights*. Springer.

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

Rosenzweig, P. (2018). Cyber warfare and the laws of war. *International Law Studies, 94*, 239-256.

Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross, 84*(846), 365-398.

Schmitt, M. N. (2012). "Attack" as a term of art in international law: The cyber operations context. In C. Czosseck & M. Ziolkowski (Eds.), *4th International Conference on Cyber Conflict* (pp. xx-xx). Tallinn: NATO CCD COE Publications.

Schmitt, M. N. (2012). International law in cyberspace: The Koh speech and the Tallinn Manual juxtaposed. *54 Harvard International Law Journal Online*, 13. https://ssrn.com/abstract=2189127

Schmitt, M. N. (2014). Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross*, *96*(893), 189-206. https://international-review.icrc.org/articles/rewired-warfare-rethinking-law-cyber-attack

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schmitt, M. N., & Billingsley, L. (2014). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Taddeo, M. (2018). *The ethics of cyber conflicts*. London: Routledge.

Appendix-A

There are a number of international treaties and agreements that have to do with the role of international humanitarian law in cybercrimes. Here are some examples:

Convention on Cybercrime also called the Budapest Convention, is the first international treaty to deal with cybercrime. It was passed by the Council of Europe in 2001, and many countries from all over the world have signed and ratified it.

Additional Protocol II to the Geneva Conventions: This protocol gives victims of non-international armed conflicts even more protection. It has rules about how civilians and soldiers should be treated, as well as rules about the use of force and the way wars should be run.

United Nations Charter: The UN Charter is the main treaty that makes up the United Nations. It lays out the rules of international law that govern how states should act. It has rules about the use of force and the fact that aggression is wrong.

The Geneva Conventions are a set of treaties that set the rules for how armed conflicts should be handled in terms of international humanitarian law. They protect civilians, people who are prisoners of war, and hurt or sick soldiers.

Convention on Certain Conventional Weapons: This treaty bans or limits the use of some weapons that are thought to hurt too many people or hurt everyone the same way. It has rules about landmines, weapons that can start fires, and laser weapons that can blind people.

Rome Statute of the International Criminal Court: This treaty sets up the International Criminal Court, which has the power to judge the most serious crimes of international concern, like war crimes and crimes against humanity. It has rules about the use of force, how civilians should be treated, and how fighting should be done during armed conflicts.