Volume 28, October 2023 ISSN 2581-5504

"Cyber Warfare Vis A Vis International Humanitarian Law"

Ankit Kumar
PhD Scholar

Abstract

The expansion of cyber-attacks is a direct result of how technological progress has rendered states, societies, and individuals completely reliant on computers, internet, and related systems. Cybercriminals' relative ease, low cost, and lack of risk have all played a role in the dramatic rise in cyberattacks in recent years. An increasing number of critical infrastructures, such as hospitals, electric power grids, water dams, nuclear power plants, and oil and gas installations, rely on computers, putting the general public at risk of catastrophic cyberattacks. Whether or not international humanitarian law applies in cyber-attacks and how to identify the attackers are two major questions that have not been resolved in this area. This study will not delve into the method of cyber attacker identification; rather, it will concentrate on the most contentious and unresolved issue of our time: the application of international humanitarian law (IHL) to cyber-attacks.

Key Words: Cyber-attack, cyber warfare, international humanitarian law, armed conflict, technological advancement.

Introduction

> "We worried for decades about WMDs – Weapons of Mass Destruction. Now it is time to worry about a new kind of WMDs – Weapons of Mass Disruption."
>
> — *John Mariotti*

Conflicts and battles have always had a major impact on how history unfolds. From the ancient Mesopotamian wars to the present-day Syrian conflict, the impact of wars on our world is undeniable. Despite claims to the contrary, most wars only serve to spark new conflicts. As the years go by, so-called civilized nations continue to wage war, with ever-increasing sophistication in weaponry and tactics leading to increasingly horrific battlefield conditions and increasing casualties.

Warfare by means and warfare by objectives are the two main categories into which the various forms of warfare that we have been observing fall. Kinetic, biological, chemical, nuclear, intelligence-based, and network-based forms of warfare are all part of the former, while economic, command-and-control, electronic, and psychological forms of warfare are covered in the latter. The military of today is significantly deadlier than its predecessors. Huge civilian casualties are likely to occur in the near future as forces engage in combat with one another. On the other hand, modern militaries are looking into less brutal and more technological forms of combat, such as cyberwarfare, which can be viewed as a form of "non-kinetic" warfare that involves electronically disrupting the enemy's communication systems or erasing its bank accounts.

Volume 28, October 2023 ISSN 2581-5504

Nowadays, the Internet is the quickest method for finding any kind of information on the planet; best solution that people consider looking into. While there are many positive aspects of the internet, such as the ability to communicate, view advertisements, download music and movies, send and receive emails, use instant messaging, and research problems, there are also many negative aspects. Internet scams and frauds come in all shapes and sizes, so it's important to be very careful. Since the advent of the internet, this has been a source of concern for both individuals and organizations; unfortunately, even the most naive among us can fall prey to seemingly innocuous situations.

Developments in technology across all domains will, as is often said, have far-reaching consequences for all aspects of society. Technological progress, particularly in the realms of communication and information, has wreaked havoc and opened up new opportunities for all types of people, including criminals. Many cyber-crimes are perpetrated with the help of the internet, computers, and cell phones, according to today's crime reports. Conversely, lawmakers have been forced to pass specialized laws to address crimes perpetrated using relevant technology. The term "computer" is defined as "any electronic magnetic, optical, or other high speed data processing device or system which performs logical arithmetical and memory functions by manipulations of electronic magnetic or optical impulses and all input, output, processing storage, computer software, or communication facilities which are connected and related to the computer in a computer system or computer network" under the statute that governs information technology in 2000. Thus, national security has grown so important in the information age that an individual can launch an assault with relative ease and in little time at all using only a computer and an internet connection. All people on Earth are in danger because of this.

They say the world has shrunk to a global village, but in reality, nations are attacking each other in an effort to gain control of the other's economy, whether out of pure aggression or a desire to protect themselves. As a result, there are new obstacles to overcome in the fight against this kind of warfare, as well as in the drafting of laws that have long been influenced by national needs and international morality.

A new danger to peace, like devastating wars, arises with the arrival of technological advancements and the addition of the new domain of cyberspace. Today, any Indian company can do business anywhere in the world with an Internet connection, supporting countless jobs and opportunities for Indians. Cyberspace and the technologies that enable it allow people of every nation, race, faith, and point of view to communicate, cooperate, and prosper like never before. A mother's ability to sell her wares to a family in Latin America from her home in rural Africa contributes to global economic development. With the help of North American software developers, hardware manufacturers in Asia, and video conferencing technology, a European lab can produce ground-breaking research while students in the Middle East and Australia study side by side. And with the rise of information technology, people all over the world are more equipped than ever to demand transparency and accountability from their governments.

Volume 28, October 2023 ISSN 2581-5504

In this day and age, when governments and individuals alike tap into the ubiquitous networks, we are presented with an option. We have a choice: give in to vested interests and unnecessary fears that impede development, or cooperate to help them achieve their full potential for increased wealth and safety. To guarantee that innovation keeps thriving, driving markets, and improving lives, cybersecurity is not an end in itself but rather a responsibility that our governments and societies must voluntarily assume. Crime and aggressiveness that existed offline have moved online, but we will fight them in a way that respects our fundamental rights to free expression, association, privacy, and information.

No longer is the internet a frontier unto itself, reserved for a select few. Responsible, fair, and peaceful behavior between states and peoples has started to take root there. As a result of the democratic collaboration between civil society, academic institutions, the business sector, and governments, it is one of the best instances of a community self-organizing. Most importantly, since its creation, this space has grown, evolved, and promoted openness and security. This is the unique quality of the Internet that makes it stand out in the global context and highlights the significance of its protection.

Efforts to implement various cybersecurity measures on a global and national scale would benefit greatly from a definition that makes a clear distinction between cyber-crime and cyber-attack. Cybercrime, cyberattack, and cyberwarfare are distinct concepts that must be understood in order to achieve this goal. The widespread and illegal use of computers and the Internet to conduct a variety of criminal acts is collectively known as cybercrime.

Individuals rather than states commit computer intrusions, store and share child pornography online, engage in fraudulent practices on the Internet, and so on, according to FBI units addressing cyber-crime. By definition, an act is considered a cyber-crime when it involves a non-state actor, is punishable by state law, does not interfere with the normal operation of a computer network, and is not driven by political or national security concerns.

The term "cyber-attack" refers to any attempt to compromise a computer network in order to achieve political or national security goals. The goal of any cyber-attack, whether it's hacking, bombing, cutting, infecting, etc., must be to compromise or interrupt the operation of a computer network. As long as the consequences don't surpass those of an armed attack, state-sponsored attacks on computer networks for political or national security purposes are considered non-conflict related.

That is why the 2011 Chinese government assault on the Falun Gong website, which involved operating a predator drone in Pakistan through a Nevada computer network, was not a cyber-attack but rather a form of technologically advanced conventional warfare. When conventional explosives are used to cut the underwater cables that transmit data packets across continents, it is referred to as a cyber-attack. Although not all cyber-crimes involve cyber-attacks, some do. Conversely, cyber-warfare is defined as an assault that takes place entirely online. However, not every cyberattack qualifies as cyberwarfare.

Volume 28, October 2023 ISSN 2581-5504

For an attack to be considered cyberwarfare, it must have consequences similar to those of a traditional "armed attack" and take place during an armed conflict. As a result of enhanced cyberwarfare, a fifth functional domain—cyberspace—has been recognized, joining the more conventional land, air, sea, and space. The United States Army, Navy, and Air Force all work together under the US Cyber Command, which was established to coordinate cyber operations. Additionally, the critical issue is whether the cyberwarfare creators or the technical individuals directly involved in the cyberattack should be regarded as combatants in this type of warfare. Another question is whether the principles of Jus ad Bellum, such as legitimate authority, just cause/right intention, possibility of success, proportionality, and the last resort, apply as much in cyberspace as they do in the real world.

This thesis examines cyberattacks through the lens of jus ad bellum, the body of law governing the use of force by states. The central argument of the thesis is that cyber-attacks are no different from any other kind of attack under the current rules on the use of force, which include the UN Charter's Article 2(4) and Article 51 as well as the relevant rules of Customary International Humanitarian Law. To illustrate the issue, we will look at a few examples of cyberattacks: the 2007 attacks on Estonia and the 2010 discovery of the malware Stuxnet, which targeted Iranian nuclear facilities.

The thesis begins with a brief historical overview of the development of the just war doctrine and the regulation of war before moving on to the main question of whether and when cyber-attacks can be considered uses of force or armed attacks. The thesis contends that cyberattacks, although being a relatively recent phenomenon with some distinctive features, are nonetheless an integral element of the development and progression of armed conflict.

Assessing whether a cyberattack constitutes a use of force or an armed attack is the subject of this thesis, which examines three methods: instrument-based, target-based, and effects-based. The most suitable perspective is the effects-based one. Cyberattacks that result in casualties, property damage, or total destruction are said to constitute the use of force. In light of the fact that cyber operations enable even without resorting to physical force, bring about significant economic repercussions; the issue of economic force is also addressed. Although it is commonly believed that economic force is not covered by Article 2(4) of the UN Charter, this view could change in the event of cyberattacks that have far-reaching consequences, leading states to reevaluate their approach to the issue.

Now we'll talk about armed attacks, and the thesis says that cyber operations could be considered armed attacks as well. In line with the commonly held belief that there is a difference between acts of force and armed attacks, the thesis asserts that cyber-operations cannot be considered an armed attack unless their consequences are extremely severe. Some contend that a denial of service attack, for instance, does not constitute an armed attack that crosses the line into legitimate self-defense since it does not cause fatalities or severe damage or destruction.

Volume 28, October 2023 ISSN 2581-5504

Cyber Attack on Nuclear Plants Control System

Nuclear power stations are another potentially harmful facility. Potentially devastating harm to people and their possessions might result from a cyberattack on this facility. A cyberattack on a nuclear power plant has the potential to cause radioactive leaks, which could cause radiation sickness, psycho-trauma, loss of life, economic chaos, and widespread property damage (Maurizio et al. 2012). Aside from the obvious external damage and loss, the attacked state stands to lose a lot more if the cyberattack wrecks its nuclear plant. As an example, the stuxnet virus was unsuccessful in its mission to destroy all centrifuges in the FEP at the Islamic Republic of Iran's uranium enrichment facility at Natanz, which it attacked in late 2009 and early 2010. The press has reported that the United States and Israel launched the stuxnet attack, which destroyed over a thousand centrifuges (David et al. 2010). The majority of commentators, including Michel N. Schmitt, eventually came to the conclusion that the stuxnet virus constituted an armed conflict because it physically destroyed around 1,000 IR-1 centrifuges at the uranium enrichment facility in Natanz, necessitating their replacement. Initially, many commentators argued that international humanitarian law (IHL) would not apply to such a cyberattack in the absence of a kinetic attack (Droege 2012: 547). As the first known case of a combined conventional and cyberwar for the purposes of international humanitarian law (IHL), the August 2008 cyberattack on Georgian networks is illustrative. Since the assault on Estonian networks did not escalate into a full-scale war, international humanitarian law (IHL) does not apply (Zhang 2012: 801).

Although cyber assaults do not directly harm the physical infrastructures of the installations in question, they do interrupt their normal operation, which in turn poses a serious risk to the public and could result in substantial financial losses. The effects of these nonlethal forms of combat may not be comparable to those of conventional kinetic weapons, but they may be just as, if not more, devastating than conventional bombing and shelling. As an example, one could attack hospital computer systems, shut down banking systems, interrupt gas and oil pipelines, cause trains to collide, manipulate the electrical grid management system, etc. At this technological juncture, every peace-loving state faces a significant danger from cyberattacks on power grid management systems, since the operation of every important installation is dependent on electricity. When power outages affect the entire state, it will put a halt to all government operations, computer systems, trains, planes, hospitals, telecommunications, nuclear power, banking, and more. There will be no actual harm to the power grids from the attack, but the human toll in terms of suffering and loss will be enormous.

According to Lin (2012: 524), the question of what constitutes an armed attack in cyberspace is brought up. is that if a cyber attack causes the same effects as a kinetic attack that rises to the threshold of an armed attack, the cyber attack will itself be considered an armed attack. Schmitt (2011: 6) opines that cyber operation, like any other operation, is an attack which may result in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.

Volume 28, October 2023 ISSN 2581-5504

The study found that the effects or consequences of a distinct cyber attacks in certain cases may be more dangerous and devastating in compare to the traditional warfare. It also found that where the scale and effect of devastation of a cyber attack is equal to or more than that of a kinetic warfare there cyber attack amounts to an armed conflict or when cyber operations cause severe damage to the property and cause death of individuals, it amounts to an armed conflict.

Conclusion

The paper concludes by stating that international humanitarian law applies in the specific context of cyber attacks that escalate into armed conflicts. As soon as a cyberattack results in substantial destruction of property and casualties among human people, it is considered an armed war. Multiple casualties and extensive property damage might result from cyberattacks on critical infrastructure such as nuclear power plants, electric power grids, water dams, air traffic control systems, and completely automated subway control systems. The United States, the United Kingdom of Great Britain and Northern Ireland, and Australia are among the several nations that have declared that international humanitarian law (IHL) applies to cyber warfare in light of the consequences of such operations (Koh 2012). Regarding the implementation of international humanitarian law (IHL) in cyberwarfare, China maintains that all countries should fight against the militarization of the internet and respect cyberspace, the first social space ever established by humans. According to it, cyberspace is not exempt from the present United Nations Charter, the rules of armed conflict, or the fundamental principles of international humanitarian law pertaining to war and the use or threat of force (Zhang, 2012). Various national perspectives, expert judgments, and the aforementioned reasoning suggests that cyberwarfare or cyberattacks that constitute an armed conflict are subject to international humanitarian law.