Spring 2023

The Exigency and How to Improve and Implement International Humanitarian Legislations More Advantageously in Times of Both Cyber-warfare and Cyberspace

Shawn J. Lalman
Embry-Riddle Aeronautical University, lalmans@my.erau.edu

Scholarly Commons Citation
Lalman, Shawn J., "The Exigency and How to Improve and Implement International Humanitarian Legislations More Advantageously in Times of Both Cyber-warfare and Cyberspace" (2023). *Doctoral Dissertations and Master's Theses*. 749.
https://commons.erau.edu/edt/749

The Exigency and How to Improve and Implement International Humanitarian Legislations More Advantageously in Times of Both Cyber-warfare and Cyberspace

Shawn J. Lalman

Embry–Riddle Aeronautical University

Submitted to the Worldwide Campus

in Partial Fulfillment of the Requirements of the Degree of

Master of Science in Cybersecurity Management and Policy

01/22/2023

Abstract

This study provides a synopsis of the following topics: the prospective limiters levied on cyber-warfare by present–day international legislation; significant complexities and contentions brought up in the rendering & utilization of International Humanitarian Legislation against cyber-warfare; feasible repercussions of cyber-warfare on humanitarian causes. It is also to be contended and outlined in this research study that non–state actors can be held accountable for breaches of international humanitarian legislation committed using cyber–ordnance if sufficient resources and skill are made available. It details the factors that prosecutors and investigators must take into account when organizing investigations into major breaches of humanitarian legislation committed in cyber–space, as well as the jurisdictional components of transgressions of the rules and L.o.A.C (*Legislation of Armed Conflict*). Due to the limitations imposed by both time and space, the planned analysis cannot be thorough; rather, it will have to remain conservative and concentrate on providing a basic grasp of the topics that are most pertinent to the modern practice of statecraft. Furthermore, given the technical and statutory complication of the subject matter as well as the fact that legal research remains in its infancy, the aspiration of this study should remain low to distinguishing matters and placing those in framework. It cannot be the goal of this study to magisterially resolute the prevailing issues that have arisen.

Keywords: cyber-warfare, international humanitarian legislation, cyber–ordnance, cyber–space, cyber combat, customs of war, Legislation of Armed Conflict, Unrestricted warfare, hybrid warfare

Contents

Introduction

One of the most significant dangers that humanity faces today is that of cyber-warfare. Cyber Warfare is an electronic attack that is carried out against nations, governments, and individual citizens that results in harm that is comparable in impact to that of a physical attack is the definition of this threat. Kinetic attacks generally inflict apparent damage to tangible structures. However, in June of 2010, a computer virus infiltrated an Iranian nuclear testing site, forcing the centrifugal pumps there to detonate (Easttom, 2018). This is a unique exception to the rule, as cyber onslaughts often do not do any direct harm.

Regardless of the apparent illustration of exerting a kinetic implication on a target, there are currently no regulations that dictate how well a government might indeed legitimately retort to such an incident. Cyber onslaughts have been increasing in frequency and magnitude over the last several years (Adonis, 2020; Deibert, 2018; Stitilis et al., 2017; Zahra, Handayani, & Christianti, 2021). N.A.T.O. (*North Atlantic Treaty Organization*) and E.U. (*European Union*) and other multilateral organizations need to come up with strategies to protect its members from the danger posed by this risk (Stitilis et al., 2017). It would be a good idea to build a framework for identifying when cyber onslaughts transcend the threshold from being an attack to becoming an act of warfare as a first step toward a constructive direction (Stockburger, 2018). Humans, policies, and procedures make up the components of a framework, which are used to quantify activities and select appropriate response measures (Schmitt & Watts, 2015). Until a methodology can be built, it is first crucial to figure out if a cyber onslaught can pass the barrier and escalate into an act of aggression. Considering legislation or policies have not yet been formed to help determine whether a cyber onslaught quantifies to an act of aggression, qualifications to solidify these criterions must be specified utilizing preexisting statutes and regulations.

When talking about combat, it is essential to talk about International Humanitarian Legislation (I.H.L), which is also known as the L.o.A.C. The I.H.L., which was formed from the Geneva Conventions, is apposite to all circumstances of combat situations and serves as the authoritative source for evaluating whether or not a certain action constitutes an act of aggression (Voitașec, 2015). The I.H.L. is accountable for establishing the present criteria of what can equitably be deemed an act of aggression. In accordance with the I.H.L., an act of war is any action that results in the death of, injury to, or damage to civilian property (Schmitt & Watts, 2015; Sohail, 2022). The I.H.L. has been subject to criticism on the grounds that it is outdated, unclear, and open to rendering. The Private and Public Sectors, Armed Forces and Civilian Segments, National and Transnational Segments, and even Organizations Such as the I.C.R.C. ("*International Committee of the Red Cross*") and the U.N. Human Rights Council (Which Do Not Represent Any Nation); contribute Significantly to the ambiguity the Humanitarian Legislation was pieced together from a wide variety of sources, some of which were in direct conflict with one another (Schmitt & Watts, 2015). This led to a great deal of confusion that exists today; the inadequacies are significant considering the fundamental purpose of the legislation: avoiding superfluous or inequitable slaughter and preserving all individuals from barbaric treatment (Schmitt & Watts, 2015; Sohail, 2022).

The lack of a consensus on what constitutes cyberwarfare only exacerbates the situation. Because cyber acts often do not involve a kinetic component, it is uncertain whether or not I.H.L applies to them (Schmitt & Watts, 2015; Sohail, 2022). The current framework for international legislation is flawed due to the fact that cyber-warfare was not taken into consideration when it was developed (Eichensehr, 2015; Stockburger, 2018). It is possible for nations to deceitfully manipulate misunderstandings regarding the cyber world in order to achieve their political and military objectives. However, developing new international legislations is a challenging endeavor, as it can take years or even decades of discussion to secure permission from a number of different nations (Eichensehr, 2015; Schmitt & Watts, 2015).

Because of the exponential rate at which technology advances, there is now a reality in which it is increasingly difficult for international legislation to continue to be applicable. In order to formulate a response, legal systems are forced to employ legislations that were drafted long before the relevant technology was developed. I.H.L offers two responses to occasions where technology improvements have developed a new type of weapon (Eichensehr, 2015). The first weapon can be considered unique, necessitating new regulations to define or forbid its use (Eichensehr, 2015). On the second point, the court may rule that the armament conforms to the common law concept of warfare and that its usage requires only minor modifications to the interpretation of current legislation. (Eichensehr, 2015). This is an outcome that is favorable to the government. Both the legality of nuclear bombs and unmanned aerial vehicles have been called into question and investigated before being found to be in compliance with the legislation. For many years, the same method has been applied to cyber-warfare, and it has always resulted in the same kind of outcomes.

Statement of the Problem

Joining the more conventional "ground," "water," "air," and "spatial" spectrum, A "5th" spectrum of warfare has emerged as the armed–forces increasingly rely on information and communication technologies. The magnitude that preexisting I.H.L. may be translated to the cyber–sphere is called into doubt by this development. There is little question that current international legislation controls state operations wherever they are executed, as well as in cyber–domain and cyber-warfare (ICRC, 2020). The enigma emerges, because to the unique qualities of the technological advances, it may be challenging to integrate established I.H.L legal norms, conceptions, and language into Cyber-warfare and Cyberspace.

Provinces whose economies are heavily dependent on the web are more vulnerable to the risks posed by cyber-warfare (Cohen et al., 2016; Eun & Aßmann, 2016). Cyber–space and technological advancements are at the point where it has invaded many facets of day–to–day life, including the infrastructure that is essential to society. This danger arises from the fact that a hostile could launch a cyber onslaught with the intention of disrupting or destroying the resources that civilians rely on (Cohen et al., 2016; Izycki & Vianna, 2021). In lieu of this, there isn't a uniform stipulatory exactness of “Cyber-Warfare”, nor is there a clear demarcation amongst an attack and an act of war. Both of these issues need to be resolved (Izycki & Vianna, 2021). In midst of the fact that policies have been drafted to mandate the strengthening of critical infrastructure systems like energy systems, such policies are only concerned with mandating that private energy providers safeguard their infrastructure rather than receiving any assistance from the government in this regard (Droege, 2012; Izycki & Vianna, 2021; Jarmakiewicz, et al., 2017; Stitilis et al., 2017).

The core issue is that cyber onslaughts actions carried out by governments, such as those involving interference with critical infrastructure, still haven't been designated by the global system as an occurrence that satisfies the requirements of an act of aggression (Izycki & Vianna, 2021; Schmitt & Watts, 2015; Schmitt M. N., 2018). This is the root cause of the issue. The significant issue is that the N.A.T.O and E.U does not have a framework for quantifying cyber onslaughts operations (Stitilis, Pakutinskas, & Malinauskaite, 2017; Wallace, 2018) conducted by a nation against energy systems, communication systems, etc., which are elements of critical infrastructure. In order to assess whether or not such activities satisfy the criterion for being considered an act of aggression; The explicit activities committed in cyber–space that can be legally recognised as an act of warfare, need to be quantified in order to build an adequate framework (Izycki & Vianna, 2021; Eun & Aßmann, 2016; Schmitt M. N., 2018). Only then can a suitable methodology be developed.

This present study will provide a synopsis of the following topics: the prospective limiters levied on cyber-warfare by present–day international legislation; significant complexities and contentions brought up in the translation and utilization of Humanitarian Legislation to Cyber Warfare; the feasible repercussions regarding cyberwarfare on humanitarian causes. Due to the limitations imposed by both time and space, the planned analysis cannot be thorough; rather, it will have to remain conservative and concentrate on providing a basic grasp of the topics that are most pertinent to the modern practice of statecraft. Furthermore, given the technical and statutory complication of the subject matter as well as the fact that legal research remains in its infancy, the aspiration of this study should remain low to distinguishing matters and placing those in framework. It cannot be the goal of this study to magisterially resolute the prevailing issues arisen.

It is also to be contended and outlined in this research study that non–state players can be held accountable for breaches of I.H.L. committed using cyber–ordnance if sufficient resources and skill are made available. It details the factors that prosecutors and investigators must take into account when organizing investigations into major breaches of humanitarian legislation committed in cyberspace, as well as the jurisdictional components of transgressions of the rules and Legislation of Armed Conflict. It discusses the applicability of several speculations of individual criminal culpability for war crimes to crimes perpetrated by non-governmental players during cyber-warfare and outlines specific evidential issues resulting from the characteristics of cyberspace and cyber–ordnance. New approaches to the application of legal concepts and ideas during cyber combat are needed if individuals are to be held to account for war crimes committed during cyber operations.

In conjunction to this research paper these research questions were brought to light in hopes of addressing;

- The question of how far preexisting international legislation can be translated into the cyberspace.
- How much, if any, cyber actions can be viewed as a danger or use of military in violation of international legislation.
- Cyber-warfare, as established by International Humanitarian Legislation, must be distinct from cyber–crime and cyber–terrorism, which are not always subject to I.H.L. Where does I.H.L. apply?
- Is the use of needed and fair force in self–defense justified in the event of a cyber onslaughts, which some call an armed attack

Methodology

The determination if the repercussions of cyber onslaughts on a state's critical infrastructure satisfy the criteria for aggression under the modern definition under the I.H.L, was the principle of said research. The objective of the study was to specify whether or not those consequences satisfy the criterion for an act of aggression. The topic of this research, namely determining whether or not cyber onslaughts may be categorized as acts of war, was a difficult sociopolitical problem to investigate. The outmoded language of the I.H.L was a major contributor to the complexities of these issue (Schmitt & Watts, 2015). The fact that such a wide variety of people, including lawyers, military officials, legislation makers, and private sector firms, have collaborated to the rendering of the legislation further complicates the situation (Schmitt & Watts, 2015). The solution to the issue can be arrived at solely via the use of numerical data, regardless of the fact that it is somewhat intricate (Liles, 2012; Schmitt & Watts, 2015). For this reason, a quantitative study that did not involve any experiments was selected.

Symbology of Research

The quantitative study was comprised of a number of different factors. The goal was to have the parameters cover any collateral harm that may have occurred, such as casualties, injuries, or property destruction with a monetary value. The non–experimental research was conducted on empirical data collected from previous occurrences that caused significant devastation. The purpose of this was to assure that there will be sufficient data to measure, and to do so, reviewing data and research papers from all around the globe. Known cases of cyber onslaughts that took a vital infrastructure down will be analyzed, along with other triggers such as power surges, financial, scheme (program), and hardware failures, natural catastrophes, cyber–related occurrences, and any other occurrences that may have caused an offline occurrence in the past (Droege, 2012; Izycki & Vianna, 2021; Sanders, 2018).

At this point in time (at the time of conducting this study), there are no international legislations or procedures in place that define a cyber onslaught as an act of aggression(war) (Sanders, 2018). The International Humanitarian Legislation and the Geneva Conventions, which are the principles that govern warfare, have become obsolete in the sense of cyber–space (Droege, 2012; Izycki & Vianna, 2021; Sanders, 2018; Stockburger, 2018). The procedure for modernizing existing legislations and regulations is drawn out and laborious, with the possibility that its completion will take more than ten years (Eichensehr, 2015). The international community may receive immediate relief from the lack of direction if actions of cyber-warfare were defined in accordance with the rules that are already in place. It is essential to ascertain whether a contemporary cyber-attack, in particular one directed at the essential water or power segments, is proficient of satisfying the present standards for an act of warfare under the I.H.L. (Eichensehr, 2015; Izycki & Vianna, 2021; Sanders, 2018; Schmitt M. N., 2018).

This study investigated whether or not cyber-attacks on critical infrastructure may be categorized as an official act of war, as well as the method by which this can be done. This will provide a road forward for future studies to be conducted in this subject. The formulation of a framework to assist nations in identifying whether such nations are legally entitled to react against a cyber-attack with a kinetic or cyber retaliation is something that should be prioritized (Sanders, 2018). The establishment of a framework provides nations with the ability to ascertain whether or not a cyber onslaught constitutes an act of warfare. A framework of this kind will prove useful to international bodies like N.A.T.O and E.U when it comes to the formulation of policy for the countries that make up their membership (Stitilis et al., 2017; Voitașec, 2015).

Once a nation has established whether or not an act of war has indeed been executed, they are in a position to protect themselves or take proper retaliatory action.

Inclination of Research (Literature Review)

The methodology for this research was quantitative and non-experimental in nature. A quantitative analysis is one that takes into account certain preset factors and seeks to ascertain whether or not there is a significant association amongst them (Creswell & Creswell, 2018). Quantitative research focuses on the numerical data that is produced as a result of testing two or more variables simultaneously (Creswell & Creswell, 2018). This provides the researcher with the ability to construct a study that is either going to support or reject a theory. The competence of the researcher to minimize prejudice and the capability of creating a study that can be reproduced are two major benefits that come from carrying out a quantitative investigation (Creswell & Creswell, 2018).

For the sake of this literature review, non-experimental quantitative approaches were the method that was going to yield the best results. When a researcher employs this methodology, the experiment is not developed and carried out by the researcher themselves (Creswell & Creswell, 2018). Rather, quantitative data is gathered by methods that do not need experimentation, such as gathering empirical data from previous events (Creswell & Creswell, 2018). In other words, this data is not collected experimentally. It was decided to go with this layout to cut down on the potential for sociopolitical bias, which can arise when dealing with a contentious topic like cyber-warfare. The collecting and examining of historical data acquired from incidents that have occurred in the past was the primary focus of this research.

Conjectures & Research Questions

The motivation behind this research is to assess whether or not an attack on a nation's vital infrastructure constitutes an act of warfare under the I.H.L. description of an act of warfare, which is "the incidental loss of civilian life, injury to civilians, damage to civilian objects, or any combination thereof caused by the actions of another nation." (ICRC, 2020; Schmitt & Watts, 2015). Hence, in order for this incident to be regarded as an act of aggression, this research needs to offer confirmation that a cyber-attack by itself can induce at minimum one of the three cases cited by I.H.L. (Creswell & Creswell, 2018; Schmitt & Watts, 2015). For the purposes of this study, a past scenario cyber onslaught will be taken into consideration in which critical infrastructure is destroyed entirely and/or how Cyberspace technology was used in conjunction with any other forms of nations aggression.

Theoretical Basis

The fact that people's personal, cultural, and religious beliefs can vary greatly, leading to a wide variety of worldviews, is the root cause of the sensitivity that surrounds this subject (Clayborn, 2021). As there are currently no intercontinental frameworks in place, it is up to individual nations to decide for themselves which kind of cyber onslaughts can be contemplated an act of aggression at this time. The following is an explanation of what is meant by the term "cyberwarfare" in the context of this study: hostile armed procedures that take place in the sphere of cyberspace (Faga, 2017). The distinction amongst cyberwarfare and cyberespionage, which are both conducted through the use of cyber-attacks, is one more element that contributes to the topic's already complicated nature (Faga, 2017). The act of stealing information, such as confidential data or intellectual property, is what is meant when talked about cyber espionage

(Faga, 2017). Cyber terrorism and cyber hacktivism are two more phrases that should be familiar, but they will not be discussed much in depth in this thesis.

Since it is impossible to wage warfare on a player like an individual, a terrorist group, or Anonymous if they are not representing the interests of a state, the notion of an acts of aggression is further complicated by the distinction amongst acts done by governmental and non-governmental players (Buchan, 2016). In accordance with stipulations of the 1949 Geneva Convention (Buchan, 2016), the lack of insignia, a command structure, or weapons demonstrates that many groups do not conduct similarly to a military. (Buchan, 2016); as a result, these organizations are ineligible for legal status as combatants. Because of the anonymity that an internet attack provides, it may be difficult to determine whether the attacker was acting on behalf of a government or a non-government organization. It is of the utmost significance for a nation to know with absolute certainty who attacked them before they can carry out any kind of retaliation action against that nation. If the attacker is successful in carrying out the covert deployment of the attack, it will be hard to ascertain who they are or the location from which they are executing.

The Research

The principle of the investigation was to conduct a critical analysis of the existing corpus of literature concerning the extensiveness and depth of wisdom on cyberwarfare. This research employed a comprehensive approach, reading academic papers that constitute each and every facet of information (Cyber) warfare, and interpreting the findings. It was determined to be the most effective method for conducting research on this subject compounded by the fact that the notion is not uniformly characterized and is seen as a complex sociopolitical issue.

The study was broken up into a few sections, the most important of which are the Significant Researchers, Chronicled Context, and Journals Studied sections. The primary analysis of the academic literature that was pertinent to the investigation was broken up into two segments. The first illustration was the utilization of cyberattacks that nations have carried across the course of history. The analysis of the study intended to determine the various implications that are presently being made of cyberattacks, as well as the extent that those various operations might or might not necessitate an act of warfare. The transnational policies and legislation that administer combat are the subject of the second field of investigation. This segment's objective was to investigate all existing intercontinental statutes that are pertinent to the waging of hostilities in order to assess whether or not those rules can be applied to cyberattacks. Because numerous of existing regulations were so incredibly out of date, few nations need not believe that they can depend solely on them to determine whether or not a cyberattack constitutes an act of aggression.

Queries Conducted on Titles, Publications, Academic Papers, and Journals

When carrying out the research for the publications comprising the research study, certain search terms, such as cyber-warfare, international humanitarian legislation, cyber–ordnance, cyber–space, cyber combat, customs of war, Legislation of Armed Conflict, and hybrid warfare, were employed as search parameters. Unrestricted warfare and hybrid warfare are concepts that are utilized to characterize strategies that incorporate physical and digital assaults in order to achieve a triumph in an armed confrontation. The Geneva Convention, the International Humanitarian Legislation, the United Nations Charter, the N.A.T.O Charter, and the Tallinn Manual were all pertinent words for writings dealing with the policy and legislation of combat. In addition to bringing up examples of cyberwar, the phrase "cyberwarfare" also resulted to publications on the legislation governing warfare. The material that was used in this literature research came from a variety of sources including media coverage, releases by the administration, internet, books, journals, and dissertations. For such purpose of this investigation, scholarly and peer-reviewed sources were sought out through the utilization of search engines. These are some of the search engines that were utilized: Google Scholar, Taylor & Francis Online, JSTOR, HeinOnline, and ProQuest.

The majority of the resources that were utilized in order to gain comprehension for this literature study were academic in nature. These sources included articles that were subjected to peer review as well as dissertations. This research made use of material from a wide variety of journals, as well as those dealing with legal topics, military affairs, cybersecurity, and/or other security-related topics. There were a few sources discovered outside of the academic world in books and news pieces. Despite the fact that these resources have little or no intellectual standards, they are a crucial component of this paper. Because of the fast-shifting social context and the ongoing technological advancement, recent events should be represented in this study utilizing resources that are more contemporary.

The Far Preexisting International Humanitarian Legislation Translated into The Cyberspace and Cyber Warfare

Cyberspace

The term "cyberspace" is commonly used to describe the worldwide system of computer systems, server farms, and other digital technologies that together form the Internet and other similar systems (Schmitt M. N., 2018). It is a virtual space where individuals, organizations, and states can interact and exchange information, conduct business, and engage in other activities.

Cyberspace has transformed the way we communicate, work, and access information. It has brought people from around the world closer together and has made it easier to access information and communicate with one another. However, this interconnectedness has also created new security risks, as cyber-attacks and other malicious activities can have far-reaching consequences (Izycki & Vianna, 2021). One of the key characteristics of cyberspace is its global reach (Izycki & Vianna, 2021; Schmitt M. N., 2018). The Internet allows individuals to communicate and access information from anywhere in the world, making it a truly global platform. This has had a profound impact on the way we conduct business, as companies can now reach customers in different parts of the globe more easily than ever before.

Another key characteristic of cyberspace is its anonymity (Shackelford, 2017). Individuals can interact and exchange information without revealing their true identity, which has both positive and negative implications. On the one hand, it allows individuals to express themselves freely and protects their privacy (Faga, 2017). On the other hand, it makes it easier for individuals to engage in malicious activities, such as cyber-attacks and cybercrime, without being held accountable for their actions (Faga, 2017).

Cyberspace has also created new security risks, as cyber-attacks can have far-reaching consequences. Cyber-attacks can take many forms, including data theft, disruption of services, and destruction of critical infrastructure (Faga, 2017; Stitilis et al., 2017). Stolen of sensitive data, disruption of key services, and even loss of life are all possible outcomes of such attacks, which can have far-reaching effects on individuals, businesses, and even entire nations (Deibert, 2018; Faga, 2017; Stitilis et al., 2017). The increasing reliance on technology has also created a new type of security challenges, as countries must now protect their critical infrastructure and military systems from cyber-attacks. This has led to the development of new security strategies and the creation of specialized units within military and intelligence organizations to defend against cyber-attacks.

One of the main challenges in protecting cyberspace is the lack of international legal framework for regulating cyber activities (Faga, 2017; Stitilis et al., 2017). While there are international treaties that govern the use of force, such as the U.N Charter, these agreements were written before the advent of cyber technology and do not address the unique challenges posed by cyber-attacks (Faga, 2017). In recent years, there has been a growing recognition of the need for international legal norms and agreements to govern the use of cyberspace (Deibert, 2018; Izycki & Vianna, 2021; Kovacs, 2018). A thorough analysis of the existing foreign law that applies to cyber operations, including the L.o.A.C, humanity rights legislation, and humanitarian law, is provided in the Tallinn Manual on the International Norms Applicable to Cyber Operations (Faga, 2017; Schmitt & Watts, 2015; Zahra & Christianti, 2021).

Despite these efforts, there is still a lack of consensus on the norms and rules that should govern cyberspace. Some states argue that existing international law and norms are sufficient, while others argue that new legal norms and agreements are needed to address the unique challenges posed by cyberspace (Zahra & Christianti, 2021). In addition to these challenges, there is also a lack of capacity and resources for many countries to defend themselves against cyber-attacks (Russell, 2014). This disparity in capabilities creates a situation where some countries are more vulnerable to cyber-attacks than others, and can lead to imbalances in the distribution of power and influence in cyberspace.

Cyberspace has revolutionized the way we communicate, work, and access information. However, this interconnectedness has also created new security risks, as cyber-attacks can have far-reaching consequences. The global community must continue to work towards developing an all-encompassing legal framework that protects individuals, organizations, and states from the effects of malicious activities in cyberspace.

Cyber-Warfare

Cyber warfare indicates the utilization of networks of technological devices and the Internet to conduct hostile and destructive acts against an opponent's critical infrastructure, government, military, and civilian population (Clayborn, 2021; Izycki & Vianna, 2021). With the increasing dependence on technology and the proliferation of connected devices, cyber warfare has become an increasingly significant security threat, both to individuals and to nation-states. These attacks can have significant consequences, including the loss of sensitive information, the disruption of critical services, and the potential for physical harm.

Cyber-attacks can take many forms, including data theft, disruption of services, and destruction of critical infrastructure (Clayborn, 2021; Faga, 2017). These attacks can have far-reaching consequences, ranging from economic loss to the disruption of critical services, such as healthcare and emergency response systems. The anonymity and global reach of the Internet make it particularly challenging to attribute cyber-attacks to specific actors and hold them accountable (Clayborn, 2021). This lack of accountability has made cyber warfare a particularly attractive option for nation-states and non-state actors, as it provides a low-risk and potentially high-impact means of conducting hostile acts.

The lack of an intercontinental legal framework for regulating cyber warfare has also been a challenge (Clayborn, 2021; Faga, 2017). While there are international treaties that govern the conduct of armed conflict, such as the Geneva Conventions, (Clayborn, 2021; Faga, 2017; Sanders, 2018; Schmitt & Watts, 2015) these agreements were written before the advent of cyber technology and do not address the unique challenges posed by cyber warfare.

In recent years, there has been a growing recognition of the need for intercontinental legal norms and agreements to govern the conduct of cyber operations.

Cyber warfare also has the potential to have a pro-found impingement on the traditional rules and norms of warfare. The decentralization of information and the ease of accessing digital tools and infrastructure have made it easier for non-state actors to conduct cyberattacks, which can blur the distinction amongst state and non-state actors and challenge traditional notions of sovereignty. Cyber warfare is carried out by nation-states and is typically highly organized and coordinated (Clayborn, 2021; Stitilis et al., 2017). The methods used can range from simple malware infections to highly complex and sophisticated attacks that use multiple methods and techniques to achieve their goals.

Despite these efforts, there is still a lack of consensus on the norms and rules that should govern cyber warfare. Some states argue that existing intercontinental law and norms are sufficient, while others argue that new legal norms and agreements are needed to address the unique challenges posed by cyber warfare. One of the main challenges in regulating cyber warfare is defining what constitutes an act of cyber aggression. There is currently no international agreement on what constitutes an act of cyber aggression (Clayborn, 2021; Schmitt M. N., 2018), and this ambiguity has made it difficult to hold states accountable for their actions in the cyber domain.

Another challenge is the double-usage nature of many cyber tools & technologies (Clayborn, 2021). The same tools and technologies used for defensive intentions can also be utilised for offensive intentions, making it difficult to distinguish amongst peaceful and hostile acts in the cyber domain. In addition to these challenges, there is also a lack of capacity and resources for many countries to defend themselves against cyber-attacks.

This disparity in capabilities creates a situation where some countries are more vulnerable to cyber-attacks than others, and can lead to imbalances in the distribution of power and influence in the cyber domain.

While cyber warfare has become an increasingly significant security threat, there is still a lack of consensus on the norms and rules that should govern this form of warfare. Cyber operations are difficult to control due to their complexity and the breakneck pace at which they evolve, but the international community must persist in its efforts to create a comprehensive legal framework that safeguards civilians and governments from the repercussions of cyber warfare.

International Humanitarian Law (I.H.L.)

The L.o.A.C are a body of principles designed to protect civilians and noncombatants from the worst of what war may bring. This legal code, which is binding on all states, is derived from a number of sources inclusive intercontinental treaties, conventional intercontinental statute, and general principles of statute.

I.H.L.'s goals are to limit the severity of conflict and to ensure the safety of civilians. Civilians, POWs (prisoners of war), the ill and injured, and aid workers are all afforded protections under this framework (Schmitt & Watts, 2015). It also mandates that all sides in a conflict identify civilian targets apart from military ones and take reasonable efforts to protect civilians and civilian property (Adonis, 2020; Schmitt M. N., 2018; Voitașec, 2015). Conflicting parties must be competent to characterize amongst citizens and non-militarization items on the one hand, and militarization of objectives on the other (Adonis, 2020; Schmitt M. N., 2018; Voitașec, 2015), in order to uphold the concept of distinction, which is fundamental to international humanitarian law. Only assaults on military objectives are allowed; attacks on civilians and civilian infrastructure are never permitted. Any ancillary damage to commoners (citizens) or noncombatant infrastructure during an assault must be proportional to the expected concrete and direct military advantage, according to the concept of proportionality (Schmitt M. N., 2018; Voitașec, 2015).

Another key principle of I.H.L. is the prohibition of unnecessary suffering (Voitașec, 2015; Wallace, 2018). This means that weapons and methods of warfare must be chosen in such a way as to minimize harm to civilians and non-combatants, and to avoid unnecessary suffering. For example, weapons that cause unnecessary suffering, such as poison or expanding bullets, are prohibited by I.H.L.

Also covered by I.H.L. are regulations for caring for war prisoners as well as injured and ill members. POWs must be handled with dignity and respect; they should never be harmed or humiliated in any way. The distressed and ailing must be aided for, regardless of their nationality or status (Adonis, 2020; Schmitt M. N., 2018; Voitașec, 2015). Another important aspect of I.H.L. is the protection of humanitarian workers, who are essential for providing assistance to those in need during armed conflicts (Adonis, 2020; Schmitt M. N., 2018; Voitașec, 2015). Humanitarian workers must be allowed to perform their duties without interference and must be respected and protected.

I.H.L. is applicable in all armed conflicts, regardless of the cause or the parties involved. It applies equally to intercontinental militarized disputes, in which two or more states are in armed conflict, and non-intercontinental armed conflicts, which occur within the province of a single state and necessitate non-state armed groups (Adonis, 2020; Schmitt M. N., 2018; Voitașec, 2015). I.H.L. is not only relevant during armed conflicts, but also in situations of occupation. Occupying powers are required to respect the laws and customs of the occupied territory, to protect the rights of the local population, and to ensure their basic needs are met. There are several treaties that make up the body of I.H.L., including the Geneva Conventions and their additional protocols, as well as other treaties dealing with specific aspects of armed conflict such as the etiquette on unequivocal customary armaments (Buchan, 2016). The I.C.R.C. perform a pivotal function in promoting and monitoring compliance with I.H.L. Despite the existence of I.H.L., violations continue to occur during armed conflicts around the world. In order to address these violations, there are several mechanisms in place to hold perpetrators accountable. The International Criminal Court (I.C.C.) has jurisdiction to prosecute individuals for war crimes, genocide, crimes against humanity, and crime of aggression ~ including grave breaches of I.H.L (Buchan, 2016). Furthermore, domestic courts have the authority to investigate and prosecute violations of warfare breaches within their borders or by their own citizens (Buchan, 2016).

Humanitarian law is essential in safeguarding civilians and non-combatants from harm during times of war (ICRC, 2020). The participants are obligated to differentiate between military and civilian targets and to exercise all reasonable efforts to avoid harming people, and the framework offers protection for civilians, POWs, the afflicted and sick, and humanitarian workers (Buchan, 2016; ICRC, 2020). It is critical to make certain that the requirements of I.H.L. are respected and enforced, and to prosecute perpetrators of breaches accountable, irrespective of the fact that they continue to persist despite the presence of I.H.L..

Interlacing I.H.L, Cyberspace and Cyber Warfare

International Humanitarian Law (I.H.L.) is a legal code that administers the usher of hostilities and sought to limit the effects of war on civilians and non-combatants (Buchan, 2016; ICRC, 2020). It is an important part of intercontinental laws that provides a framework for protecting civilians during times of conflict. As the world becomes increasingly dependent on technology and with the evolution of technology and the growing use of cyber means in warfare, the question of how I.H.L. applies to cyber operations has become increasingly relevant.

The application of I.H.L. to cyber warfare is a complex and evolving area, as the laws and principles that have been developed over the years are still being adapted to the unique challenges posed by cyber operations. Some of the key issues that arise when considering the application of I.H.L. to cyber operations include the definition of armed conflict, the distinction amongst civilians and military objectives, and the application of the principle of proportionality (Adonis, 2020; Buchan, 2016). Cyberspace is also a new domain of warfare that has introduced new challenges and complexities to the application of I.H.L.. One of the main challenges is that cyberspace operates in a virtual environment that is not confined by geographical borders, making it difficult to attribute responsibility for cyberattacks to a particular state or nonstate players (Adonis, 2020; Buchan, 2016; Stitilis et al., 2017). This has led to concerns about the lack of accountability for violations of I.H.L. in cyberspace

The definition of armed conflict is a crucial aspect of I.H.L., as it determines the extent to which I.H.L. applies in a particular situation. In order to apply I.H.L., it must be established that an armed conflict exists, which can take the form of either an intercontinental armed conflict amongst states, or a non-intercontinental armed conflict amongst a state and a non-state armed group, or amongst non-state armed groups (Adonis, 2020; Buchan, 2016; Schmitt M. N., 2018; Stitilis, et al., 2017). The definition of armed conflict in the context of cyber operations is still a matter of debate, but it is customarily sanctioned that I.H.L. administer to cyber operations that have a significant and direct impact on the physical realm and that cause harm to individuals or objects protected under I.H.L.

I.H.L. places a strong emphasis on differentiating the goals of civilians and those of the armed services, this is an additional significant feature of I.H.L. This dichotomy is essential to International Humanitarian Law since it determines the guidelines for targeting in times of warfare. Numerous cyber activities are capable of having civilian and military implications, therefore distinguishing respectively civilian and militaristic aims is not always straightforward in the context of digital operations. Quantitative analysis must be performed on each prospective civilian and military target, taking into account the particulars of the objective as well as the environment in which it is situated (Adonis, 2020; Buchan, 2016; Creswell & Creswell, 2018). Another dilemma is that the repercussions of cyberattacks can have a far-reaching and substantial impact on the civilian population, potentially causing damage to fundamental infrastructure and services such as health-care, power generation, and transportation. This is a dilemma because the repercussions of cyberattacks could have a substantial impact on the civilian population. These poses problems concerning the responsibilities of nations to ensure the security of civilians in cyberspace as well as the degree to which I.H.L shields civilians from the impacts of cyberattacks.

Despite the challenges posed by the application of I.H.L. to cyber operations, there are also some important similarities amongst cyber operations and traditional armed conflict that can inform the application of I.H.L. to cyber operations. For example, the principles of distinction and proportionality that apply to traditional armed conflict can also be applied to cyber operations (Buchan, 2016; Droege, 2012; Zahra & Christianti, 2021). Additionally, the rules on the protection of civilians and nonmilitary objects during armed conflict can be adapted to the specific challenges posed by cyber operations.

The Tallinn Manual on the Intercontinental Statute Applicable to Cyber Operations (Roscini, 2019; Zahra & Christianti, 2021) provides a detailed study of the present-day Intercontinental Laws that relates to cyber operations, including I.H.L. Humanitarian law principles such as protecting minorities, protecting civilians, and protecting cultural property are discussed, along with their potential application to cyber operations (Zahra & Christianti, 2021).

Initiatives have been launched by international bodies like the I.C.R.C. to advocate the applicability of I.H.L. to cyberspace (Zahra & Christianti, 2021). The I.C.R.C. has urged the creation of a cyberspace legislative framework that adheres to the norms of I.H.L. and guarantees the preservation of citizens and noncombatants during military confrontation.

However, despite these efforts, there is still a lack of consensus on the norms and rules that should govern cyberspace in times of armed conflict. Some states argue that existing I.H.L. norms and principles are sufficient, while others argue that new legal norms and agreements are needed to address the unique challenges posed by cyberspace (Droege, 2012; Stitilis et al., 2017; Zahra & Christianti, 2021).

The application of I.H.L. to cyber operations is a complex and evolving area, and there is still much debate over how I.H.L. should be adapted to the unique challenges posed by cyber operations (Zahra & Christianti, 2021). However, there are some important similarities amongst cyber operations and traditional armed conflict that can inform the application of I.H.L. to cyber operations, including the principles of distinction and proportionality, as well as the rules on the protection of civilians and nonmilitary objects during armed conflict (Droege, 2012; ICRC, 2020; Stitilis et al., 2017; Zahra & Christianti, 2021). As technology continues to evolve and the use of cyber means in warfare becomes increasingly prevalent, it will be important to continue to adapt I.H.L. to the complex and evolving cyber domain.

Cyber Warfare as a Tactic

This segment is meant to confer diversified uses of cyber attacks across history. To increase their chances of success in conflict and warfare, military commanders have been exploiting technological tools since ancient times. Initially, these techniques were implemented to back up more conventional forms of kinetic combat. The significance of these strategies has increased drastically alongside the development of technological tools, and they are therefore capable of functioning as a separate act of combat in their own respect (Zahra & Christianti, 2021). This portion will also compare and contrast the differing tenets of Western and Eastern perspectives on warfare and the employment of cyberattacks, which contribute to a muddled understanding of the topic. This portion will show why it's important to formalize the concept of cyberwarfare and amend existing international norms to reflect this reality.

Keeping up a strong military forces costs a lot of money for any country. Countries can maintain their military relevance and competitiveness by constant modernization of infrastructure and the substitution of older technologies for newer technologies (and if called upon – reuse old tech). Participation in the actual war, even at a preliminary level, would increase domestic debt and bring countries to the brink of economic catastrophe. Non-material expenditures, such as diplomatic, psychological, and emotional costs, will plague the nation for decades after a war's conclusion, in addition to the obvious financial and material tolls (Colarik & Janczewski, 2012). Involve yourself in the idea of cyber warfare. There is no denying the potency of cyber weaponry. They have both offensive and defensive applications and produce military outcomes that are often similar to their physical world counterparts (Colarik & Janczewski, 2012).

Furthermore, Armaments of the Cybersphere pose a threat in ways to the armed forces resources of the adversaries, but also in ways to the strategic state goals, such as economic and political networks. Even the smallest cyber-attack can temporarily cripple a nation's infrastructure, population, and mental health when the complete spectrum of cyber threats is considered (Colarik & Janczewski, 2012).

Cyber weapons, which are readily available, have been promoted as an alluring substitute for conventional weaponry. When engaging in cyberwarfare, you can't just randomly attack random targets in cyberspace. Government, military, and people in many countries are only loosely connected. These countries tend to be poor and lack scientific advancement. Such a disconnected nation would feel little to no effects from a failed cyberattack and might not even recognize it (Colarik & Janczewski, 2012). Armed forces have the advantage that everyone under their command can employ the weapons at their disposal. The effectiveness of a cyber attack against a population that is not highly connected or dependent on computers is low. One cannot just reply with force to every attack; instead, one must show some degree of accountability for the challenges that one faces. For this reason, it is crucial to determine the scope of actions and ensure that they align with a geostrategic security interests.

Conventional weapons require constant upgrading and eventually become obsolete, but this does not mean that war has to be prohibitively expensive. Cyber weapons, which can be quickly and cheaply produced and deployed, would enter the conflict at this point. While most weapons of this type can be controlled, certain cyber weapons cannot.

Cyber Warfare at “Infant” Stage

On January of 1904, during the Russo-Japanese Warfare, an early instance of cyberwarfare occurred in the Suez Canal (Evans, 2018). The British ship HMS Diana was able to effectively intercept a wireless signal sent by the Russians (Evans, 2018). It is believed that the British and their ally Japanese were able to prevail in the battle thanks in large part to their capacity to intercept Russian signals (Evans, 2018). The idea of communications intelligence was developed as a result of this occurrence. This type of cyberwarfare is known as signals intelligence, and it refers to the act of intercepting and possibly manipulating communications that are taking place amongst personnel or equipment (Evans, 2018). Any and all forms of data that are sent digitally amongst humans and/or machines can be considered part of these exchanges. Even though the use of signals intelligence somehow doesn't meet the requirements to be considered an act of aggression, the fact that it gives the side that employs it a unique edge should not be overlooked.

The United Kingdom (U.K.) started developing RADAR, an early alert system to spot approaching enemy aircraft, in secrecy in the 1930s (Evans, 2018). The British were able to dispatch interceptor fighters in time to avoid harm because to RADAR's ability to foresee and track impending strikes (Evans, 2018). The development of RADAR was essential in changing the course of WWII. During WWII, radio signals were developed to help direct bombers to their nighttime targets (Evans, 2018). The Germans were initially more successful in combat thanks to these advanced technologies (Poirier & James Lotspeich, 2013). Nevertheless, the Allies figured a how to interrupt German transmissions and take control of them. By diverting the bombers into ambushes and even detaining some of aircraft, the Allies were able to stop them from destroying their targets.

During the War of Latakia, which took place in 1973 (Evans, 2018), Israeli missile boats were ambushed by Syrian warships armed with Russian missiles just outside the harbor (Evans, 2018). Technological preventative measures were utilized by the Israeli military, which was adept in disrupting the missile navigation systems and resulting in the missiles missing their targets. This is an illustration of how defending against a cyberattack can be utilized to bestow a strategic advantage. The technology, on the other hand, is completely useless for anything other than a kinetic assault.

The United States of America and a select number of its allied forces began hostilities against the nation of Iraq in the Gulf War during 1991 (Brenner, 2011). This constituted a chance for the United States to demonstrate its technological capabilities and its tactical dominance on the battleground. The deployment of an experimental '*Global Positioning System*' in a military setting is one illustration of this technological capabilities in action (Brenner, 2011). Whilst the use of this technological knowledge resulted in a swift triumph, it also brought to light the dangers of relying too much on advanced technologies to win battles, a fact that was observed by the United States' opponents, notably China.

Cyber Warfare at "Adult" (Contemporary) Stage

The Russian government initiated a series of Distributed Denial of Service (D.D.o.S) assaults targeting Estonia in April 2007 (Evans, 2018; Russell, 2014), deeming Estonian administrative, commercial, and financial sites inaccessible for 3 weeks (Russell, 2014). The assaults on Estonia were reprisal for the nation's decision to remove a monument honoring Russian World War II veterans (Russell, 2014). Whilst this is prime illustration of a nation-state waging war via cyberspace, under current international law it fails to constitute an act of aggression because no lives were lost and no infrastructure was destroyed.

To prevent the Syrian government from detecting an impending airstrike in September 2007, Israel attempted a cyberattacks targeting Syrian radar equipment (Dwyer, 2018). It wasn't until 2018 that Israel finally revealed the publicized their acknowledgement about the matter

(Dwyer, 2018). Although it was never conclusively shown, prior to this most analysts believed that Israel was responsible for the cyber-attack on Syria (Dwyer, 2018). As opposed to Russia's distributed denial of service attacks on Estonia, this incident has indeed been recognized as the inaugural incident of contemporary cyberwarfare by a small subset of industry professionals. Cyberwarfare can be circumscribed as the use of cyber aptitudes to gain an advantage over an adversary. Because the cyberattack did not cause any deaths or damage on its own, it cannot be classified as cyberwarfare apart from the kinetic airstrike.

Cyberwarfare was arguably first used in the confrontation involving Georgia and Russia in 2008 (Russell, 2014). As soon as Georgia declared its independence from Russia, Russia launched an assault (Russell, 2014). The Russian methods in Georgia were much more advanced than in Estonia, and the cyberattacks were accompanied by a physical invasion. Similar to the situation in Syria, cyberattacks weren't considered an act of war until they were used to augment traditional military operations. During the onslaught on Estonia, there was no military struggle to speak of, which seen as a key difference amongst the 3 instances (Schmitt & Watts, 2015).

Russia's use of both physical and digital assaults has been labeled a "hybrid war," (Russell, 2014) which also includes political and psychological operations. Hybrid warfare is said to be executed with precision and can be carried out in a variety of ways. The Russian military said it needed this new approach because kinetic combat was no longer effective in certain conditions (Russell, 2014; Schmitt M. N., 2018). Russia excels at hybrid warfare because it is ingrained in the country's military culture. In 2009, Russia would use the same tactic of combining conventional military force with cyberattacks against Kyrgyzstan again (Evans, 2018). Additionally, in 2014, they used composite (hybrid) warfare in the Ukraine in an effort to topple the incumbent government there and stop the nation's secession (Evans, 2018).

Cyberattacks, propaganda, guerilla tactics, and physical violence were all used to achieve this goal. Russia's use of hybrid warfare in Ukraine failed to achieve its goal, but it did succeed in sparking a confrontation that lasted for several years.

Warfare Not Governed by China's Restraints

With intercontinental nations taking the superiority of the potency of technological warfare, China sort this as an opportune time to “jump into the game” of “Cyberwarfare” (Altamura, 2020). Cyber domain tech that is not specifically geared toward warfare is also a focus for Chinese. Additionally, all categories of commercial, medical, and pharmaceutical technology are being gathered together (Altamura, 2020). This technique not only makes rapid technical growth possible, but it also enables China to enter foreign trade marketplaces, which hurts the economies of the nations from which intellectual property was stolen in the first place (Altamura, 2020). The combination of this technique with the high number of cybercrimes that are being committed by them has caused some analysts to label China as the most significant threat to global information security. Despite the fact that these actions do not now fit the criteria for an act of war, China's status as a global powerhouse is strengthened as a result of them, and the target countries suffer as a result. This is a distinction that has to be understood thoroughly because it demonstrates the possibility for nations to exploit the vacuum of norms and regulations governing the execution of cyber-attacks.

Chinese Cyber Warfare – Operation Gh0stNet

The People's Republic of China conducted a global cyber-espionage operation codenamed "Operation Gh0stNet." (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). Diplomatic governments, embassies, humanitarian bodies, media outlets, and non-governmental organizations are just some of the myriad victims that Chinese cyber troops have attacked and stolen data from, totaling over one-hundred-and-three regions (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). A total of approx. 1300 hosts in over 100 nations were effectively attacked and compromised by PRC cyber-espionage forces; this cyber intrusion happened within a 2-year timeframe amongst from 2007-2009 (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013); this number includes hosts in the politically contentious province of Tibet. As its stated goal, the malware-based cyber-espionage network's primary objective was to steal information about Tibetan assets around the world (Altamura, 2020). A number of non-governmental organizations (NGOs) operating in Europe and North America, as well as the Private Office of the Dalai Lama, were singled out as targets of the "Gh0stNet" operation (Altamura, 2020). Infected machines were instructed by Gh0stNet to execute the malicious payload gh0st RAT, which gave hackers full control of the compromised machines in real time. "Gh0stNet" took control of affected machines, allowing for the theft of sensitive data and the activation of remote devices like microphones and webcams. It was discovered that the "gh0st RAT" virus originated from corporate Internet access accounts that were based on the Chinese island of Hainan (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013).

One might be puzzled how the cyber operators compromised so many Dalai Lama-affiliated computers and kept them that way for so long. Consolidation is the key, since it allows hackers to utilize the data stolen during one cyber espionage operation to launch attacks on additional computer systems. This maybe thought of this as the fourth stage of a four-phase process (stages are ordered to listing):

- ➢ *Reconnaissance* entails stage 1 actions including footprinting, scanning, and enumerating to identify potential entry points into the system.

- In stage 2, *exploitation* stage, cybercriminals steal from or otherwise tamper with the information/data of their intended victims.
- Keep remaining *persistent* is stage 3, which essentially means staying on the target system without being detected by the software and peripherals.
- *Consolidation*, stage 4, takes part of the data gleaned during exploitation and uses it to make new targets.

"Spear phishing" is a technique used in cyberattack tactics, like the one carried out against the Dalai Lama's organizations, in which hackers employ social engineering to send emails that appear to come from a trusted source but really include malicious software (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). The cyber spies who infiltrated the Tibetan exiles' computers first sent out enticing e-mails in the hopes that many of their recipients would click on a link and download a virus (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013).. Users were tricked into downloading a malicious Trojan by a message that appeared to come from a trusted source and was formatted in Microsoft Word. Afterwards, highly targeted emails were sent out, with data gleaned from the victims who activated the original Trojans.

Nonetheless, there is yet another facet of security protocols that should be thought about, and that is technology. How do the system administrators identify potentially harmful files, and where do they send them to be quarantined? Hackers frequently try to leverage lesser-known system vulnerabilities in supplement to discovering such methods in the reconnaissance phase of the operation cycle. After analyzing harmful files discovered on the computers of Tibetan businesses, researchers discovered that just Eleven of the Thirty-four top anti-virus program in use at the time correctly identified the files as carrying Trojans (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). Cybercriminals can easily gain access to computer networks and avoid technical protection mechanisms like antivirus software by taking advantage of lesser-known weaknesses or even developing new ones.

Chinese Cyber Warfare – Operation Gh0stNet; Acquisition of Data on Undermine Networks

The computers of the Tibetan refugees were infected with at least eight distinct Trojan families. After the virus connected to its command server, it granted full access to the compromised machines. The software deployed by the Trojan will first establish communication with a command & control (C & C) server. Researchers found that over seventy–% of C & C servers were located in the PRC (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). Besides Taiwanese, the United States, Scandinavia, S. Korea, and others all hosted command and control servers (Shakarian, Shakarian, & Ruef, 2013). Not only that, but the HTTP protocol was being utilized for communications with these C & C servers. With this common protocol, the data traveling to and from these servers is less likely to raise red flags with network intrusion detection systems.

The investigators discovered that a number of the C & C servers they had previously identified were still up at the time of the study (Shakarian, Shakarian, & Ruef, 2013). Investigative team members were able to infer the C & C server's file structure from the servers' apparent setup (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013).. Using this line of thinking, they tracked out the machine's remote administration software and hacked its control panel. The infiltrated computers may be controlled by the hackers via simple Web-based displays utilizing the software's management interface. It was determined that the researchers' theory was accurate after further investigation (Shakarian, Shakarian, & Ruef, 2013). To make matters stranger, they discovered unprotected administrator interfaces on 4 of the C & C servers. This gave them complete control over several of the infected machines.

Each C & C server's management interface consisted of a trifold display. Among these was a directory of infected computers that were talking to the server, a command-sending interface, and a screen displaying the executed instructions (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). The instrument that could issue commands to the targets was flexible. The acquired system data may include a document listing from the target machine, further malware could be sent to the target to expand its capabilities, and the virus could be made inactive using one of the other features (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). With the capacity to transfer more malware to the target, the hacker may gain access to the target's file system, screen, microphone, and webcam, as well as manipulate files on the target and record keystrokes, keystrokes, and audio. The extra malware's executable code is masked as an image file during transmission to avoid detection.

The Chinese program gh0st RAT is one of the extra malware variants that may be sent to a victim's computer via the command & control server (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). Several of the features (key logging, file management, etc.) made it possible because the hacker is granted real-time access to the targeted system (Shakarian, Shakarian, & Ruef, 2013). It is important to remember that gh0st RAT may be set up to communicate with an external C & C server. Having a second master server might be a red herring or an attempt to divide and conquer in terms of processing requests for the target.

The researchers sought to know more about how the gh0st RAT version on the Buddhists' networks communicated with their command & control servers (Shakarian, Shakarian, & Ruef, 2013). They use a device called a “honey pot” to attract the “black-hats” (cybercriminals) they need (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). A computer set up as a honey pot is intentionally made to look weak in order to attract hackers. Cyber-Experts in the field of cyber defense will keep an eye on the intruders' behavior once they've gained access to the honey pot. The researchers, nonetheless, decided to install gh0st RAT on their own honey pot instead of waiting for it to get infected (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). In the wake of its installation, the honey pot used by the researcher sought to connect to Chinese master servers. The Chinese computers may have only been conduits in the scheme, as gh0st RAT is capable of using proxy servers. Listing of files and folders, as well as the physical location of the target system, and information about the target system (memory, disk space, machine name, OS version, etc.) are among the results (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). The cyberspy can pick and choose which program (such as gh0st RAT) to employ to further exploit the system based on the data supplied (Shakarian, Shakarian, & Ruef, 2013). With this extra information, the bad actor can make sure that any further malware transmitted to the victim will not only work, but will do so in the most covert way imaginable. Exploiting a computer is greatly aided by gaining access to a directory listing of its files and folders. As a result, a "black-hat" hacker deploying gh0st RAT or a comparable program can predetermine what information to steal from the victim machine. Hackers frequently use this strategy since it considerably enhances the likelihood that it will be discovered, as it involves actively searching through the data located on the target system in real time. Cybercriminals were also able to discover the nation an infected machine was situated in by doing a geoIP query on the target, which was made possible in some updated versions of the administrator interface (Shakarian, Shakarian, & Ruef, 2013). Accurate nation information of a system may improve spear-phishing assaults, therefore geographic data is useful not only during the exploitation phase but also when planning subsequent actions during consolidation.

Chinese Cyber Warfare – Operation Night Dragon

The Chinese government carried out a series of cyberattacks against energy businesses under the codename “Operation Night Dragon” (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). During 2011, McAfee detailed how the P.L.A. (People's Liberation Army) went after five different energy and petroleum corporations all around the world (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). The attacks made use of a variety of Windows-based exploits and trojans, in addition to extensive social engineering that targeted employees and individuals linked with the company (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). The Chinese government carried out the cyberattacks by using compromised servers in the Dutch systems (Netherlands) and hosted servers in the United States. The P.L.A. carried out attacks against corporate network architectures that contained privileged information including operational blueprints (Altamura, 2020; Shakarian, Shakarian, & Ruef, 2013). These attacks were carried out by the P.L.A. Attackers were able to successfully breach network architectures by negotiating perimeter security controls, exploiting SQL-injection flaws in extranet web servers, launching spear-phishing attacks on laptops, and compromising corporate V.P.N. accounts. This allowed them to infiltrate the defensive architectures of the targeted company and conduct reconnaissance on the networked computers of the targeted company.

Russian – Georgia August 2008 Hybrid Warfare

The Russian military invaded Georgia in August 2008 to drive Georgian forces out of South Ossetia (Easttom, 2018; Evans, 2018; Shakarian, Shakarian, & Ruef, 2013; Zahra & Christianti, 2021). The military operation was preceded by multiple synchronized cyber strikes. In the history of major land combat operations, this is the first time a coordinated cyber attack of this magnitude has been initiated. Although there is no proof that the Russian administration was involved, the cyber strikes had a profound effect on the Georgian citizens by cutting them off from the rest of the globe.

Cybersecurity analysts from a privately, nonprofit organization called the "US Cyber Consequence Unit" previously recognized 2 distinct stages to the Russian cyber assault against Georgia. Russian hackers began the first stage on the evening of August 7th, focusing particularly on Georgian media and administration websites (Easttom, 2018; Evans, 2018; Shakarian, Shakarian, & Ruef, 2013; Zahra & Christianti, 2021). Anatoly Tsyganok, (Commander of the Russian militaristic Forecasting Center), said these preliminary moves are in retaliation for Georgian cyberattacks on South Ossetian media networks previously in the week (Shakarian, Shakarian, & Ruef, 2013). It is to be noted of the date that the reported counterattacks happened just one day before the start of the ground battle. Because of this, numerous specialists in the field of cybersecurity now believe that the invaders likely had advance notice of the invasion's timeframe.

D.D.o.S cyberattacks (distributed denial of service cyberattacks), were the dominant form of intrusion that Russian hackers used during the first stage of their operation (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). During this time period, botnets were predominantly responsible for D.D.o.S attacks. Botnets are rented out and used by criminal groups like the Russian Business Network (R.B.N.) (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). The RBN & other Russian criminal groups were linked to the botnets that launched the attack on Georgian websites.

Websites associated with the Georgian press and governmental were the primary targets during this initial round of the cyberattacks. The Russian botnets used a brute-force Distributed

Denial of Service attack to take down its targets. The Georgian networks were especially vulnerable to the Russian hackers' flooding attacks because of their inherent fragility.

While D.D.o.S cyberattacks on Georgian press and government webpages persisted in the second stage of the Russian cyber operation, they aimed to harm a wider range of organizations, including banks, corporations, universities, western news outlets (including B.B.C. and C.N.N.), and even a “black hats” (cybercriminals) site in Georgia itself. Web pages defacements were a component of the wider D.D.o.S attacks on these servers (e.g., pro-Russian graffito on administration webpages such as a visualize likening M. Saakashvili ~ (Georgian President) to Adolf Hitler) (Easttom, 2018; Evans, 2018; Shakarian, Shakarian, & Ruef, 2013; Zahra & Christianti, 2021). Many Russian hackers also launched a spamming email blast using the names and e-mail accounts of Georgian lawmakers that were available online.

SQL injection is a different form of attack that the Russian hackers used in order to deface websites (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). They used this method in order to get access to the sites. This specific strategy takes advantage of a weakness that is widespread in web applications. "SQL" stands for "structured query language" and is the most widely used method for writing database schema at the present time. SQL code is injected into a Web form from an untrusted source as part of an attack known as a SQL injection (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). This code is then transferred to the back-end database of the application, where it either dumps the database or modifies the content of the back-end database (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). Any information stored in a database that is vulnerable to this type of attack can be stolen by a hacker. This includes user login credentials, banking data, and even site data.

During this stage of the assaults, the majority of the cyber activity turned its focus to the recruitment of Russian computer users who exhibited "patriotic" sentiments (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). It was believed that many people who called themselves "hacktivists" were actually members of Russian youth groups, in particular the Nashi, according to comments on certain Russian hacker websites (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013).

The acquisition was conducted mostly through a variety of websites, the most notorious of which being StopGeorgia.ru, which came live on August 9th and has since gained a lot of notoriety (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). One member of the hacktivist group remarked that the procedures that were supplied were simple enough that even a new user could follow them (Evans, 2018; Shakarian, Shakarian, & Ruef, 2013). For instance, StopGeorgia.ru offered straightforward resources and guidelines for initiating a distributed denial of service attack from local computers (Shakarian, Shakarian, & Ruef, 2013). It also had a simple button labeled "FLOOD" that, when activated (Voitașec, 2015), would launch several distributed denials of service attacks against Georgian targets. The purpose of all of these assaults was the same; they were just using various methods to do it. This included both botnet activity and hacktivist attacks (D.D.o.S): to flood Georgian servers with a brute force D.D.o.S (Shakarian, Shakarian, & Ruef, 2013). The tools that were supplied also had a high degree of adaptability. For instance, some individuals were able to concurrently attack up to Seventeen Georgian servers (Shakarian, Shakarian, & Ruef, 2013). Such hacktivist websites also offered target lists of Georgian networks, with information like whether or not the system was accessible from Russia or Lithuania, as well as details regarding any acknowledged security vulnerabilities, such as a propensity to be vulnerable to SQL injection (Easttom, 2018; Shakarian, Shakarian, &

Ruef, 2013). It is indeed interesting of mentioning that a plethora of security specialists have established a connection between StopGeorgia.ru and Russian organized crime.

The degree of competence exhibited by the operators of the Russian hacker websites is yet another fascinating characteristic of these websites. Not only did they offer helpful guidance to rookie hacktivists when it was needed, but they also performed an excellent job of monitoring their sites (Japaridze, 2020; Kelly, 2012; Shakarian, Shakarian, & Ruef, 2013; Stitilis et al., 2017). Whilst fighting commence, managers of the Russian "black hat" site "*XAKEP.ru*" swiftly replied to port-scans by an open-source security project headquartered in the United States dubbed "*Project Grey Goose*" by momentarily censoring all Internet Protocol (IP) addresses from the United States (Japaridze, 2020; Kelly, 2012; Shakarian, Shakarian, & Ruef, 2013; Stitilis et al., 2017). There was also proof that they promptly cleaned up the server. For example, in a matter of hours, they removed a post that had the keyword "ARMY." (Japaridze, 2020; Kelly, 2012; Shakarian, Shakarian, & Ruef, 2013; Stitilis et al., 2017). As it turns out, the admins' skepticism is quite well: a bogus program meant to conduct assaults targeting Georgian objectives was published to a Russian hacker domain (Shakarian, Shakarian, & Ruef, 2013). On the other hand, it was discovered that this particular piece of software was designed to attack systems located in Russia (Shakarian, Shakarian, & Ruef, 2013). Experts determined that Georgian cybercriminals were responsible for uploading the malware in an attempt at a cyber retaliation; nevertheless, no evidence was found to suggest that the program did any substantial damage.

In reaction to Russian cyberattacks, Georgia first censored access from Russian IPs (Schmitt M. N., 2018); however, the Russian hackers rapidly diversified and began using servers that were located outside of Russia or IP addresses that were falsified. After that, the Georgians relocated a large number of their sites to servers located in other countries (mainly U.S.A.). Yet, even these international servers were particularly prone to the inundation vulnerabilities because of the exceptionally large quantity of the Russian brute force attack. This was the case even if the servers were located outside of Russia.

Russian – Georgia Hybrid Warfare: The Objective of the Cyber Warfare

The Russians aimed to "detach & mute" the Georgians with their cyber operations. The attacks succeeded in;

- Silencing Georgian media
- Walled the nation off from the rest of the globe

Corbin's theory is supported by accounts of the incident and listings of potential victims posted on Russian hacker websites. In addition, the Georgian citizens suffered a major psychological and informational setback since they could not alert the rest of the globe regarding what was unfolding.

Colonel A. Tsyganok described the Russian cyber assault as part of a bigger information struggle with Georgian and western media, while being cautious not to connect the attacks to the Russian government (Shakarian, Shakarian, & Ruef, 2013). Cyberwarfare, according to Russian journalist M. Zharov, is just one component of a broader information operation that also involves bloggers and traditional media (Shakarian, Shakarian, & Ruef, 2013). Around 300K+ people who responded to a C.N.N./Gallup survey at one time said they felt the Russian cause was legitimate (Buresh, 2021; Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013).

Several experts believe the initial stage of the Russian cyber strike was designed to silence Georgian media outlets from reporting the country's side of the conflict (Buresh, 2021;

Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). This fits with Russia's focus on cyberwarfare. The assaults on Georgian banks during the second stage of cyber operations may also be explained by the aim of cutting off Georgia from the rest of the globe. Many financial institutions were hit by a wave of fraudulent activity at this period. To limit their exposure, international banks suspended business in Georgia during the conflict. The banking system in Georgia was thereafter unavailable for 10 days (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). During the second phase, Russian hackers may have also targeted Georgian company websites with the intention of causing economic harm (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013).

Nonetheless, it must be stressed that the "detach & mute" strategy had narrow goals. In most cases, Georgian networks and their associated *Industrial Control Systems (I.C.S.)* and *Supervisory Control and Data Acquisition (S.C.A.D.A.)* objectives were able to avert catastrophic cyber assaults (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). Systems like this are developed for real-time data collecting, control, and monitoring of essential utilities including energy systems, oil/gas networks, refineries, and water infrastructure (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). It's clear that the Georgian infrastructure would suffer greatly if these systems were ever disrupted. It's reasonable to infer that some caution was applied to make sure these targets were avoided, given that Russian hackers certainly had the means to activate them. Most importantly, Georgia's Network infrastructure suffered minimal disruption. Georgia had mainlined connections to the Internet via Turkish, Armenia, Azerbaijani, and Russia at the moment of the assaults (Buresh, 2021; Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). There is no indication that any effort was made to disrupt the physical or online connectivity facilitated by Russia (Shakarian, Shakarian, & Ruef, 2013). This may indicate that the Russian aggressors' goal was not to permanently cripple Georgia's Network, but rather to "isolate & quiet" certain services. Restrictions on military actions are also typical in traditional military settings. During the first stage of Operation Iraqi Freedom, for contrast, the electricity and oil grids were not attacked (Buresh, 2021; Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). Notwithstanding the hostilities, there are strong economic and cultural links between Russia and Georgia. So, irreparable harm to Georgia's Internet infrastructure might have unfavorable results for both sides.

Russian – Georgia Hybrid Warfare: Cyber Warfare Harmonization with Armed Forces

There was relatively little cooperation between cyber and conventional troops. In spite of widespread claims that Russian hackers were aware of when ground operations would begin, proof of cooperation beyond the timing of cyber strikes is sparse (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013; Stitilise et al., 2017). Other explanations include;

- The Russian administration's desire to maintain complete detachment from the cyber assault operations (even though there is yet no definite evidence)
- The Russian military's limited adoption of jointness at the time of the war, which led to cyber activities being compartmentalized.

Researchers in cyber security have noticed, nevertheless, what they believe to be signs of cooperation among cyberspace and ground forces (Adonis, 2020; Shakarian, Shakarian, & Ruef, 2013). The effectiveness of the Russian cyber strike may explain why, for instance, kinetic measures (— in other words, regular combat with firearms and explosives) weren't utilized to target communication and news infrastructures. In a more out-of-the-ordinary move, Russian hackers also targeted a website that leased diesel-powered electricity generators. Therefore, it's possible that customary operations targeting Georgian's power grid were the impetus for this particular cyberattack.

Cyber – Competence: Grooming for Disputant

The Russian campaign as a whole benefited from the cyber assaults, irrespective of whether the Kremlin was directly engaged. Because of this, cyber functionalities might be viewed as an essential component of a modern advanced warfare infrastructure, alongside movement, weaponry, air defense, and others. The study of cyberspace requires a thorough grasp of the adversary's cyber capabilities. It should recognize that the adversary hacker comes in many guises, including state-sponsored lab employees, uniformed personnel of cyber units, criminal organization insiders, and hacktivists (politically motivated hackers) (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013; Stitilise et al., 2017). While interacting with others in online, it might be tough to tell who is who. Yet knowing which cyber soldiers make up an adversary's order of battle might provide light on their strategies. After the order of battle is in place, cyber "doctrinal templates" (DOC.TEMP) can be implemented (Shakarian, Shakarian, & Ruef, 2013). If one was to take the battle in Georgia as an example, one may assume that Russian criminal groups are present in the Country, despite the fact that their precise connection to conventional troops is unknown. If one were to know that they were in the order of battle, one can investigate a DOC.TEMP linked to the offenders. It may also imply the deployment of botnets and hacktivists with the objective of isolating and silencing the adversary, without causing lasting damage to the cyber infrastructure or ICS/SCADA (Buresh, 2021; Shackelford, 2017; Shakarian, Shakarian, & Ruef, 2013).

The Georgian incident also suggests that military and civilian networks alike need to be protected against intrusion if one is to learn anything from it (Shakarian, Shakarian, & Ruef, 2013). In Georgian, Russian cyber strikes had substantial informational and psychological consequences despite not being directed at military objectives. Even more so, some cyber attacks, like the ones that occurred in July against Georgian official websites, may portend not just larger-scale cyber strikes but also ground operations (Shakarian, Shakarian, & Ruef, 2013). There may come a time when it's crucial to maintain the continued operation of civilian computer networks in order to assist defend the local inhabitants.

Thus, a commander may choose to construct cyber-centric priority information requirements (P.I.Rs) (Shakarian, Shakarian, & Ruef, 2013; Stitilis et al., 2017). Data that an army commander needs to know as quickly as possible is called "priority information requirements." A military leader would customarily make a choice in response to such data (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). Despite of the specifics of any given conflict, military leaders in the future will have to factor in the effects of cyber operations on their overall strategy.

It's possible that smaller-scale cyber assaults are precursors to more extensive cyber strikes or even physical operations. There are various warning indications of an imminent cyber assault, and the responsibility for reporting them may rest on different people. For armed services networks, computer security staff or a liaison with the government of the host country could report questionable network activity. An impending cyber attack may also be foreshadowed by bloggers or other posts on hacker websites. Open-source intelligence (OS.INT) analysts might keep an eye on such activities (Buresh, 2021). Last but not least, traditional forms of intelligence reporting like signals intelligence (SIG.INT, data collected through the interception of digital signal) and human intelligence (HUM.INT, knowledge gathered from insiders) ought to be entrusted with and trained to recognize indicators of cyber attacks unique to their domain (Buresh, 2021).

The Aug 2008 cyber campaign launched by the Russian Federation against Georgian was the first time such a large-scale cyber offensive has occurred in tandem with massive conventional warfare actions. Press and administration in Georgian, as well as the public at large, were hampered in their capacity to connect to the rest of the globe because of these cyber warfare’s, which had a profound effect on the dissemination of information and the state of mind of the population. Whereas the assaults cannot be clearly connected to the Russian government, the gains are evident and should be considered during potential future wars. A cyber-capable adversary requires adjustments to processes like P.I.Rs creation and R & S (reconnaissance and surveillance) preparation.

The Hezbollah 2006 July War

The extermination of ex-Lebanese Prime Minister Rafiq al-Hariri in February 2005 (Sobelman, 2016) sent reverberations throughout the state. The United States and France both demanded that Syrian forces leave Lebanon after this happened, and the Lebanese people responded with rallies (known "Cedar Revolution") (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). In the end, Syria complied, and in April 2005, the Lebanese formed a new coalition government (Sobelman, 2016). As a result of this new administration, the majority of the Western expected Hezbollah to disarm. Despite being designated as a "terrorist group" by the U.S.A., the Islamist militant group backed by Iranians is able to operate in Lebanon (Sobelman, 2016). Despite widespread skepticism in Lebanon, Hezbollah's leadership ultimately chose to initiate a retaliatory assault upon Israel in July 2006 after hearing rumors of an imminent Israeli attack on Lebanon (Sobelman, 2016). The group is responsible for the deaths of 3 Israeli soldiers and the abduction of 2 more during cross-border operations. Next, Hezbollah launched a barrage of short-range missile assaults towards Israel. As a response, Israel retaliated severely, killing nearly over 1K innocent Lebanese (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016) and wreaking havoc on the country's infrastructure without successfully removing the real threat, Hezbollah. Around a month into the war, the Lebanese government made the possibly escalating announcement that it would send 15K forces to the South. U.N. Resolution 1701 (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016), which called for a ceasefire and effectively ended the "2006 Lebanon War," came at a time when both parties wanted the fighting to halt.

Each parties employed a wide range of cyberwarfare tactics to complement their on-the-ground activities. Israelis notably launched a D.D.o.S attack against the websites of Hezbollah's "Al Manar" TV network. Israeli citizens, led by the "International Union of Jewish Students," developed a program dubbed "megaphone" to notify people to internet polls, message boards, and blogging where pro-Israeli content may be posted. According to competing reports, Hezbollah hackers have breached the networks of Israeli Defense Force (I.D.F.) troops stationed near the Lebanese border (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). Since there are no public allegations of D.D.o.S cyberattacks upon combat IDF forces throughout this battle, it is probable that any such activity was for intelligence collection.

Israeli Cyber Psychological Operation

The use of cyber tactics to bolster Hezbollah's intelligence activities stands out as among the most significant examples of its deployment throughout this fight. S. Hassan Nasrallah, the head of Hezbollah, was featured on the Al-Manar satellite television network encouraging people to witness the burning Israeli ship shortly after a successful missile assault on an Israeli navy vessel (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). His comments were shown after visuals of the assault and the resulting destruction. There was no confirmation of the occurrence from the Israelis at that time (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016).

Hezbollah's plan relied heavily on a multifaceted approach to cyberwarfare (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). Cyber psychological operations (CY-OP) was a crucial part of the whole. The term CY-OP refers to the use of cyberspace to conduct covert operations against military and civilian targets (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). As an illustration, one side in a conflict may employ CY-OP by spreading their message via "new media," or social networking sites like Facebook (Sobelman, 2016). Similar to how a D.D.o.S assault may be used to prevent the dissemination of an enemy's propaganda, CY.OP can be used to disrupt the enemy's communication channels. In the early 2000s, Hezbollah established a new tactic it called cybercortical warfare, and CY-OP was a crucial component of this new approach. The objective of this tactic is for a state or non-state actor to utilize its credible political and armed services strength to decree attention and project information power, therefore actively altering the data environment of a conflict via the Internet.

Several Western allies of Israel, including the United States, responded to Hezbollah's cyber operations by blocking Hezbollah-affiliated websites like Al-Manar (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). As well as physical attacks, there were rumors that the I.D.F was attacking Al Manar and other Hezbollah websites over the internet. Hezbollah "hijacked" IP addresses from companies all across the world, including the United States, Canada, and India (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016), since they did not have their own, genuine IP address. Data travels between nodes on the Internet via a network of devices called routers. The term "autonomous system" (A.S) is used to describe a group of Internet routers and other network devices that is managed by a single entity (Sobelman, 2016). Every A.S has what are called border gateway routers, which communicate with the rest of the Internet. These advanced routers interact with the rest of the Internet to properly route data destined for a device within a certain A.S. If you want to visit a company website, for instance, your request will travel over the Internet until it reaches the Company’s B.G.P router. It then goes through the Company’s internal networks to get to their website. Internet routers are able to forward the request to Business A's A.S because the company's border gateway router broadcasts the IP addresses used by the company to its neighboring Internet routers. In order to transmit this data, the "Border Gateway Protocol" is used.

The B.G.P. protocol relies on an unspoken bond of trust between peers (Sobelman, 2016). When a border router sends a list of IP addresses to a neighboring router, the receiving router takes it at face value that all of the addresses are O. K (Sobelman, 2016). IP addresses of few given to this network may be stolen (Sobelman, 2016), nonetheless, if the administrator of an independent system does not take the necessary safeguards and/or incorrectly configures the B.G.P router. In this scenario, an outside party promotes some of the addresses in the target system.

According to Time magazine's H. Hylton, stealing an IP address is like adding an extra phone line to a victim firm (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). If the victim doesn't notice the theft of their IP address, the hijackers have successfully used it for their own objectives (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). During the July conflict, Hezbollah acted in this manner. The "Society for Internet Research," (Society) who call themselves "freelance counter-terrorists," (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016) spearheaded the attempt to thwart Hezbollah's hijackings. These unofficial computer security specialists kept tabs on Hezbollah's Internet traffic, looking for the hijacked IP so they could notify the intended victim and put a stop to their intelligence activities (Shakarian, Shakarian, & Ruef, 2013). The “Society” found that when Hezbollah was discovered, it was able to swiftly “pirate” new I.P addresses, leading them to describe their exertions as "whack-a-mole" since as soon as one compromised IP address was disabled, another one was compromised very immediately (Shakarian, Shakarian, & Ruef, 2013).

Important from a cyber war standpoint, Hezbollah war of July 2006 (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016) shows how cyber warfare and information operations are becoming increasingly intertwined. Hezbollah adopted cybercortical warfare as a strategy, which led to a close linking of tactical operations with data activities. The Israeli approach of blocking their opponents' websites is reminiscent of what the Russians allegedly did to Georgian sites in 2008 (Shakarian, Shakarian, & Ruef, 2013). Yet, Hezbollah effectively retaliated with cyber operations of their own, expanding on their prior intelligence activities. Hezbollah was able to keep spreading its strategic message by continuously stealing IP addresses from innocent bystanders.

Cyber Warfare – 2008 Israel-Hamas War: Operation Cast Lead

Israelis launched "Cast Lead" in December 2008 to prevent more rocket fire from Gaza into southern Israel (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). Airstrikes on the initial day of the campaign destroyed 50 Hamas objectives (Sobelman, 2016). Israelis launched a strategically planned propaganda offensive at the outset of the conflict. The I.D.F started a YouTube channel dubbed the "I.D.F. Spokesperson's Unit" two days after the first airstrike (Shakarian, Shakarian, & Ruef, 2013). Several I.D.F. troops developed the concept for this channel, which featured vlogs from I.D.F. members, firearm recordings of targeted attacks, and film from humanitarian aid operations. The "Jewish Internet Defense Army" was also instrumental in getting Jews all around the globe to use the Online services and other "new media." (Sobelman, 2016). For starters, their webpage featured guides for making use of several forms of social media, such as Facebook, YouTube, Wikipedia, and different forms of blogs (Sobelman, 2016). In addition, they claimed responsibility for blocking access to many pro-Hamas YouTube channels, suggesting that they targeted not just traditional media but also the "new media" of the opposition side.

In response to Israel's data activities operation, Hamas and the people of Gaza created their own material exposing the destruction wrought by the Israeli bombardment (Sobelman, 2016). The citizens of Gaza were able to share their narrative with the global community because to the widespread use of cellphones, Twitter, digital photographs, and blogging. In response to efforts to take down their YouTube streams, they created paltube.com, a website exclusively to Hamas content.

Hamas and its followers not only launched their personal information campaign to counter Israeli data activities operation, however they additionally engaged in a massive graffiti effort against Israeli webpages (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). Even if certain Web site defacements were significant enough to garner press notice, the true harm (presumably economical) is thought to have arisen from the sheer quantity of activities taken by pro-Hamas cybercriminals. Pro-Hamas organisations would often use the web server program to do basic vulnerability scans on selected Israeli websites (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). Pro-Hamas cybercriminals would break into the system, then desecrate it with anti-Israeli vandalism once they had access to that area (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016).

Hamas followers have used D.D.o.S assaults, but on a smaller scale than the websites they have defaced. A pro-Hamas hacker, adapted a D.D.o.S program called al-Durrah for use in the 2008 Gaza conflict (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). Like the D.D.o.S scheme used by Russian hacktivists during the Georgian War (discussed earlier by this paper), this program made it simple for inexperienced users to join in on D.D.o.S assaults without having to hand up administrative privileges on their own machines. After downloading "al-Durrah" from a pro-Hamas hacker site (Sobelman, 2016), a client input the addresses of aimed Israelis servers into the program's interface, causing a deluge of requests that would finally bring down the server (Sobelman, 2016).

The Israeli hackers were equipped with their own D.D.o.S tools. To combat pro-Hamas websites, "Help Israel Win" developed a program called Patriot (Sobelman, 2016). Patriot users' computers would be directed to launch assaults after connecting to a C & C server with the Name "defenderhosting.com," leading experts to label the program a "volunteer botnet." (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016) Patriot is not user-configurable, therefore defenderhosting.com has full control over the cyber assault operations of its volunteer host (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016).

Throughout the course of the conflict's 24 days, the narrative swing from Israelis to Hamas grew increasingly prominent (Shakarian, Shakarian, & Ruef, 2013). Images of the destruction in Gaza quickly multiplied over the world's news outlets (Shakarian, Shakarian, & Ruef, 2013). Where did this change come from? The most plausible reason is that Israel began restricting access to Gaza by the media several months before the conflict broke out. They did this because they knew Hamas and the people of Gaza would broadcast graphic footage of confirmatory deface to infrastructure and civilian fatalities. Israel would buy more time to achieve its tactical goals if the international community took longer to call for a resolution to end the hostilities because of a decrease in the output of such reports. The I.D.F was able to accomplish its tactical aims, hence its strategy was effective (as opposed to the 2006 conflict with Hezbollah) (Shakarian, Shakarian, & Ruef, 2013). The trade-off, nonetheless, was that any news coming out of Gaza had to come from Hamas and Gazans themselves (Shakarian, Shakarian, & Ruef, 2013).

So, the narrative coming out of Gaza was biased. The Israelis effectively prevented any objective party from disproving the allegations of the Gazans by barring independent journalists from entering the region. While the I.D.F did manage to infiltrate the Hamas television station and Israeli sympathizers did attempt to "black-hat" penetrate pro-Palestinian Facebook accounts, these cyber operations were not enough to prevent Hamas from sending a powerful message to the world (Sobelman, 2016). In addition, the story of the Gazans was communicated to the whole (Arabian) globe due to the presence of Al Jazeera reporters who remained in Gaza until the I.D.F began to restrict press credentials (Sobelman, 2016).

The 2008 Israel–Hamas confrontation exemplifies the use of social media in present-day cyber operations throughout warfare and the efforts of both parties to combine cyberspace operations to promote their respective strategies (Shakarian, Shakarian, & Ruef, 2013; Sobelman, 2016). While Hezbollah's IP address hijacking was a key factor in the success of their data activities operation in 2006, neither Israel nor Hamas were able to make extremely successful use of cyber techniques to augment their particular public relations in 2008 (Sobelman, 2016). Israelis tried to prevent Gazans' tale from becoming viral by attacking a pro-Hamas website with a distributed denial of service assault and by blocking pro-Hamas YouTube channels, but they finally failed (Shakarian, Shakarian, & Ruef, 2013). Even though Hamas supporters may have used IT expertise to their advantage, they seemed unable to carry out fruitful, intricate cyberwarfare; rather, their cyber attacks seemed to be constrained to website obfuscation techniques and minor to moderate D.D.o.S intrusion. Maybe because they don't have the same level of technological skill as Hezbollah did back in 2006. This may indicate that cyber security was not a top concern for Hamas in 2008.

Laws of Warfare

The appropriate reaction of a nation to a physical attack is clearly established by international law, treaty, and historical precedent (Shackelford, 2017; Voitașec, 2015). Cyberwarfare necessitates a rewrite of antiquated rules such as the Geneva Conventions and the I.H.L. (ICRC, 2020). Many of these regulations were drafted many years before today's sophisticated computer technology and widespread reliance on computers even existed. Instead, because revising them would be a massive and time-consuming operation, the interpretation of these laws should be modified.

In the repercussion of the Second World War, the Geneva Conventions were discussed for 4 years (Voitașec, 2015) before being finalized and accepted by the Geneva Diplomatic Conference on August 12th, 1949 (Voitașec, 2015). At its foundation, I.H.L. primarily consists of the Geneva Conventions and their supplementary protocols (ICRC, 2020). The standards of I.H.L. apply to any armed conflict, regardless of whether or not a state of war has been proclaimed. The law can be categorized into two subsets: *Jus ad Bellum* & *Jus in Bello* (ICRC, 2020; Voitașec, 2015; Zahra & Christianti, 2021). What is meant by the word "jus ad bellum"? It refers to the body of law that determines when it is appropriate for a nation to employ aggression (Shackelford, 2017; Voitașec, 2015). The term "jus in bello" signifies the rules that regulate the activities that nations are permitted to perform when they are engaged in armed conflict (Shackelford, 2017; Voitașec, 2015).

Cyber activities amid hostilities are not science fiction. While only a small handful of nation-states have admitted openly to conducting such operations, a growing quantity of nations is building military cyber capabilities, suggesting that their usage will only expand in the years ahead.

In addition, cyberwarfare capabilities have advanced greatly in recent times. Cyberattacks have demonstrated the potential to have far-reaching effects on civilian infrastructure and may even lead to human casualties. The I.C.R.C. is focused with cyber operations as a medium and tactic of combat throughout military confrontation, and the safeguard that I.H.L. gives from their impacts, because this is in keeping with the I.C.R.C's purpose and mandate (ICRC, 2020; Voitașec, 2015).

Cyberspace activities have been deployed in conjunction of or in tandem with kinetic actions during times of war. Cyber-ops have the potential to present advantages unavailable through traditional techniques of combat, but they also come with their fair share of dangers. While traditional combat actions often result in collateral civilian casualties and infrastructure damage, cyber operations may offer a way for combatants to attain their military objectives without endangering noncombatants (ICRC, 2020). But contemporary cyber operations have shown that skilled adversaries have gained the power to impede the provision of critical services to the civil population. These activities are typically undertaken outside the framework of military confrontation (ICRC, 2020; Voitașec, 2015; Zahra & Christianti, 2021).

Warring parties can conduct cyber operations to gain access to a system and steal information, delete files, encrypt data, or otherwise tamper with it (Zahra & Christianti, 2021). A hacked computer system can also be used to initiate, modify, or otherwise influence operations. Companies, infrastructures, telecommunications, transportation, governments, and financial institutions are all instances of tangible "objectives" that may be disrupted, manipulated, or harmed. The latent human cost of cyber operations against essential non-combatant infrastructure, such as healthcare facilities, is a major reason for apprehension.

Critical infrastructure has become more at risk from cyber assaults in recent years. According to reports, both their frequency and severity are rising at a faster rate than was predicted by specialists (Adonis, 2020; Buchan, 2016; ICRC, 2020; Sohail, 2022; Zahra & Christianti, 2021). Furthermore, there is a lot of mystery around the most advanced cyber capabilities and technologies that have been or are being developed, the future of technological advances, and how cyberwarfare may differ from current patterns during military actions.

Likewise, cyberspace's unique properties give rise to unique worries. While conducting cyber operations, for instance, the targeted party may have trouble determining if the assailant's goal is intelligence collection or more severe impacts, increasing the potential for intensification and related human suffering. The intended objective may overreact in an effort to prevent a catastrophe it believes is imminent (Sohail, 2022).

Cyber tools also spread in their own special way. After their first application, they might be reworked for new purposes and put to widespread use by parties other from those who created or utilized them.

Many aspects of conduct in times of hostilities are governed by preexisting treaties and customary law pertaining to the armed conflict law. There is a heightened need for adherence to the legislation of warfare in cyber domain. The restrictions here are meant to shield civilians from harm during wartime. These are grounded on the supreme principle of distinction, according to which warring parties must always tell the difference amongst civilians and combatants, and also among citizen targets and military goals, and focus their efforts solely on the latter (ICRC, 2020; Voitașec, 2015; Zahra & Christianti, 2021).

Despite the interconnected nature of cyber domain, cyber technologies may be made to be selective in their effects via rigorous observation. Several of the subsequent cyber assaults that have been publicized in the media seem to have been technically "discriminate," (Adonis, 2020; Buchan, 2016; ICRC, 2020; Sohail, 2022; Zahra & Christianti, 2021) meaning that they were created and deployed with the intention of harming only specified targets. Yet, it could prove theoretically arduous and demand for meticulous planning in its conception and maturation to ensure that cyber activities harm just the intended item. Therefore, even if a cyber activity is theoretically discriminate, it does not make it legal, either beforehand or following a war.

Nonetheless, there are cyber tools that are already publicized and have the potential to spread on their own and impact numerous systems without any discernment (Clayborn, 2021). They haven't just happened to be self-replicating; that feature has to be included in during development. Due to the global nature of cyber domain, everything that can communicate with the Internet may be attacked. Furthermore, the results of an intrusion on one system may spread to other systems without discrimination. So, there is a veritable possibility that cyber tools will not be created or utilized in accordance with I.H.L.

If the concepts of distinction, proportionality, and prudence from IHL are extended to cyber activities during wars and conflicts, then the following regulations must be adhered to:

- It is forbidden to possess cyber operations that are so lethal and indiscriminate that they could potentially be considered weapons (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- The utilization of cyber instruments or tactics of warfare in direct assaults on citizens and noncombatants' infrastructure is strictly forbidden (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- Intentional actions or threats of violence against citizens, whether or not they are carried out using cyber means or traditional tactics of warfare, are strictly banned (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- Operations that do not distinguish amongst military targets and citizens or noncombatants' infrastructure are forbidden, and this includes the use of cyber as a warfare (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- Even when employing cyber apparatus or techniques of warfare, excessive assaults are forbidden. Onslaughts that have a high likelihood of causing disproportionate citizen fatalities, wounds, or infrastructures impair in comparison to the anticipated tangible and direct military benefit are considered disproportionate (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- Continual precaution needs to be exercised to save the civil population and civilian infrastructure's during combat operations, such as when employing cyber implication or methodologies of armed conflict; every reasonable measure needs to be taken to prevent or reduce accidental civil danger when launching attacks, including via cyber medium or methods of warfare (ICRC, 2020; Sohail, 2022; Voitașec, 2015).

- The employment of cyber techniques and tactics of warfare, including the onslaught, destruction, removal, or making unusable of things essential to the existence of the population, is strictly forbidden (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- Cyber activities during armed situations must be conducted with due regard for the safety of medical services (ICRC, 2020; Sohail, 2022; Voitașec, 2015).
- In addition, states already have a commitment in peacetime to take all reasonable measures to safeguard people and civilian property from the consequences of cyber means and techniques of warfare (ICRC, 2020; Sohail, 2022; Voitașec, 2015).

Separating armed services and citizen networks and framework in cyber domain, isolating critical noncombatant infrastructure's digital systems from the Internet, and collaborating to identify in cyber domain the cyber infrastructure and networks serving specially protected objects like health facilities are all possible steps to take (ICRC, 2020).

For certain military-related networks, civilians make up the vast majority of cyber domain users. It's possible, nevertheless, that armed services and civil connectivity are linked (ICRC, 2020; Sohail, 2022; Voitașec, 2015). Additionally, armed services networks might lean on noncombatant virtual infrastructure such as underwater fiber-optic cabling, satellites, routers (ICRC, 2020; Sohail, 2022; Voitașec, 2015). On the other hand, global positioning system technologies may also be utilized by the defense, but they are progressively relied upon by civilian vehicles, commerce, and air traffic controllers (Adonis, 2020; ICRC, 2020; Zahra & Christianti, 2021). Certain military communications travel through identical internet and transmission lines that are used by civilians' logistics distribution networks and important citizen services.

It is important to note that under I.H.L., a civilian item is not automatically classified as a military goal just because it is used for military objectives (ICRC, 2020). If it does, the rule against attacking civilian objects head-on no longer applies to the target. If military presence in cyberspace eventually leads to the realization that numerous items constituting part of virtual space are no longer protected as civilian objects, this becomes a very severe problem (Adonis, 2020; ICRC, 2020; Zahra & Christianti, 2021). Substantial interruption of the increasingly vital civilian use of cyberspace might result from this.

Yet, the norms of proportionality and care in assault would still apply even if some portions of the digital infrastructure were no longer shielded as civilian objects during armed confrontations. Because to the interrelated nature of civilian and military networks, it is essential to evaluate the potential for collateral civilian damage from every cyber operation (ICRC, 2020).

More and more, digitalisation platforms are relied upon by vital civilian infrastructure to deliver crucial services. For the sake of public safety, it is crucial to fortify this infrastructure and those providing it against cyber assaults and accidental harm.

Without respect to the nature of the damaging operation, I.H.L. offers special defense for particular infrastructure, such as medicinal aid and items vital to the existence of the people (ICRC, 2020). The majority of I.H.L's protections for citizens and noncombatant property originate from the concepts of distinction, proportionality, and prudence, however these rules only apply to "assault" under IHL's strict definition (ICRC, 2020). Assaults are defined as "acts of violence against the adversary, whether in offensive or in defense," according to Article 49 of Additional Protocol I (Adonis, 2020; Buchan, 2016; ICRC, 2020; Stitilis et al., 2017; Voitașec, 2015). The application of these regulations and the preservation they give citizens and citizen's infrastructure hinges on the query of how broadly or marginally the concept of " onslaught" is construed in relation to cyber operations (ICRC, 2020).

There is consensus that cyber actions aimed at causing demise, detriment, or physical damage qualify as assaults under I.H.L. The I.C.R.C considers this to encompass damage from both the immediate and longer-term consequences of an assault, such as the loss of life in critical care units as a result of a cyber operation on the energy grid that knocks out power to the hospital (ICRC, 2020).

Amongst the greatest threats to people, however, is posed by strikes that target key services but do not always produce physical harm. Nevertheless, opinions vary on either if a cyber-ops that results in a loss of functioning but no physical harm constitutes an onslaught as defined by I.H.L (ICRC, 2020; Sohail, 2022; Voitașec, 2015). The I.C.R.C believes that any action taken during hostilities with the intent to cripple computers or networks is an onslaught under I.H.L, regardless of whether the item is disabled using kinetic or cyber methods (ICRC, 2020). A cyber activity aimed at rendering a noncombatant system (such as electricity, financial services, or communication systems) inoperable, or expected to cause such effect incidentally, may not be protected by vital I.H.L rules protecting the civilians and civilian objects if the concept of onslaught is viewed as only attributing to activities that produce demise, harm, or physical harm (ICRC, 2020). Inconsistent with the spirit and intent of the I.H.L regulations on the behavior during war would result in an unreasonably narrow definition of aggression. Thus, it is crucial that nations come to an agreement on how to best safeguard civilian populations from the fallout of cyberwarfare.

Digitised civilizations can't function without crucial citizen data including health records, biometric identifiers, social security numbers, tax returns, financial accounts, customer profiles, and voter rolls (ICRC, 2020). Such information is crucial to the smooth operation of most facets of civilian life, both on an individual and a social scale. The need to protect this kind of critical citizen information is becoming more pressing.

Critical information, such as health center records, are included in the requirement to respect and safeguard these entities, and are thus provided some of the specialized security offered by I.H.L (ICRC, 2020; Sohail, 2022; Voitașec, 2015). Most fundamentally, humanity and civilian objects are shielded from harm by the primary I.H.L. principles and laws guiding the conduct of conflicts (ICRC, 2020; Eichensehr, 2015). Hence, it's crucial that nations come to an agreement that civilian data is shielded by these regulations.

Removing or altering crucial citizen datasets may swiftly bring government agencies and commercial enterprises to a halt. More innocent people might be harmed by these activities than would be lost in the destruction of property. Although it is not yet clear if vital noncombatant information necessitates civilian objects (ICRC, 2020), the I.C.R.C finds it hard to harmonize with the object and intention of I.H.L the assertion that erasing or manipulate with such essential civilian data would not be prohibited by I.H.L in forthwith cyber–contingent globe (ICRC, 2020; Sohail, 2022; Voitașec, 2015). The security afforded by I.H.L should not be lessened because paper files and documents are being replaced by data files stored digitally. There would be a significant protection gap if vital civilian data were excluded from the protection granted by I.H.L to civilian objects.

Accountability by other players is made more difficult by the fact that they may conceal or forge their identities using a broad spectrum of technical tools available in cyber domain. This presents very serious challenges. I.H.L (ICRC, 2020), for instance, is only applicable to activities that are related to the combat, including during periods of hostilities (ICRC, 2020).

It can prove challenging to ascertain if I.H.L. is relevant to a cyber operation if its originator (and, by extension, the relationship between the operation and a military action) cannot be recognized (Buchan, 2016; ICRC, 2020). Furthermore, crucial is the ability to attribute cyberattacks to their perpetrators so that those who contravene I.H.L and other international norms can be held to account. The prohibition upon utilizing such assaults may be weakened, and players might be less conscientious regarding utilizing them in breach of international law (ICRC, 2020), if they believe it will be simpler to disclaim culpability for such assaults (Faga, 2017; ICRC, 2020). Having stated of this, attribution is not an issue from the standpoint of the players that lead, coordinate, or command cyber operations. This is because these players have access to all of the data necessary to identify within which global regulatory structure they are acting and whose duties they are required to follow.

Weaponizing Cyber Tools Upon Critical Infrastructure

Maroochy Water Services, located on the Sunshine Coast of Queensland, Australia, was the target of the cyberattack (Shakarian, Shakarian, & Ruef, 2013). Two control centers, communicating through 3 radio channels, managed the operation of 142 sewage pumping stations in the Maroochy S.C.A.D.A system (Shakarian, Shakarian, & Ruef, 2013). S.C.A.D.A Systems like this are developed for real-time data collecting, control, and monitoring of essential utilities including energy systems, oil/gas networks, refineries, and water infrastructure (Buresh, 2021; Shakarian, Shakarian, & Ruef, 2013). Alarms that didn't make sense, increasing radio traffic, unauthorized changes to the S.C.A.D.A system, no warnings when certain things happened, and the constant hum of the pumps all contributed to the growing unease among the plant's workers. The issue, first was faulty installations (Shakarian, Shakarian, & Ruef, 2013). As enhancements had just been made to the system, this made sense. In spite of this exhaustive investigation, which included reinstalling part of the S.C.A.D.A software, the system settings were still “shifting” in mysterious ways. Reasoned that because of this, the liabilities couldn't be the consequence of some sort of accidental failure.

It was also found out that an intruder was connecting to the S.C.A.D.A system using wireless communication technology by employing monitoring devices (Shakarian, Shakarian, & Ruef, 2013). Experts in cyber security said they engaged in a "duel" with the hacker (Shakarian, Shakarian, & Ruef, 2013) at one point. It was determined that V. Boden, a previous contractor who had been rejected for employment by the Maroochy Shire Council, (Shakarian, Shakarian, & Ruef, 2013) was the hacker. For 3 months, Boden managed all 142 pumping stations using nothing more than a laptop computer and a radio transmitter (Shakarian, Shakarian, & Ruef, 2013). Throughout the course of that period, he dumped approx. a million liters of raw sewage into a storm drain (Shakarian, Shakarian, & Ruef, 2013) that ultimately flowed into nearby bodies of water. In the end, he was apprehended and sentenced to time served.

What this tragedy shows is that there are challenges to ensuring the safety of an industrial control system. To begin, it may be challenging to recognize an attack for what it is. This is due to how intricate an I.C.S (Industrial Control Systems) system actually is. Mechanical failure, incorrect settings, or incompetent operators are only some of the numerous potential causes of an unexpected error. The second reason is that insider attacks on I.C.S systems are very common (Izycki & Vianna, 2021). They often exhibit a wide variety of weaknesses (Izycki & Vianna, 2021; Shakarian, Shakarian, & Ruef, 2013), (the infrequency with which I.T. systems may be updated and patched compared to conventional ones). So, an insider is more likely to be aware of the system's weaknesses, as Boden obviously was with the Maroochy facility (Shakarian, Shakarian, & Ruef, 2013). Last but not least, the harm inflicted by such a system has a far more immediate impact on human lives than the compromising of an I.T. system. Several Sunshine Coast residents, marine life etc. were exposed to water pollution as a result of the sewage spill into the stormwater drain (Shakarian, Shakarian, & Ruef, 2013).

The Russian hackers behind ***Dragonfly*** first targeted aerospace and defense firms in the Americas in 2011 (Izycki & Vianna, 2021). Cyberattacks targeting the industrial automation systems of U.S. and European power utilities shifted focus in 2013 (Izycki & Vianna, 2021). The United States, Spain, France, Italy, Germany, Turki, Poland, Romania, Greece, and Serbia were hit particularly hard (Izycki & Vianna, 2021). The second iteration of the group's primary artifact, dubbed "Dragonfly 2.0" by Symantec (Izycki & Vianna, 2021), has been seen reportedly beginning at the end of 2015. The United States, Swiss, and Turkish were the primary adversaries in the second gen.

In the 3rd and 4th months of 2018, United States Incident Management Center and the National Cyber Security Center expressed concerns (Izycki & Vianna, 2021) about impending Dragonfly assaults on institutions such as the administration, the energy sector, the nuclear industry, water supply, air transport, and industrial output.

Server Message Block (S.M.B) credentials were stolen in this assault (Izycki & Vianna, 2021), which leveraged site breaches and spear phishing to get N.T.L.M (New Technology LAN Manage) 1 credential. N.T.L.M is a standard for authenticating users on Windows-based networks and independent computers. After the hacker has gained access to the network, they will try to bounce among workstations by employing stolen credentials, penetration testing, and other network administration techniques. According to the US Cert's forensics (Izycki & Vianna, 2021), the hackers gained entry to workstations and servers where they could see the output of control systems within electricity producing plants on many occasions.

“Darkness” That Fell Upon the Realm– Cyber Warfare Against Energy Infrastructure

For the purpose of this study, the energy/power/electricity sector should be deemed as a comprehensive Critical Infrastructure. Because simply put energy “drive” the contemporary globe.

The term "energy grid" refers to the network that links power plants to homes and businesses that use energy (Izycki & Vianna, 2021; Shakarian, Shakarian, & Ruef, 2013). Information must be communicated amongst specific places on the network to fulfill various grid needs, including as metering and fault location (Izycki & Vianna, 2021). This calls for a wide range of information technologies (I.T). The electricity grid's present I.T technology for communication includes both cutting-edge and antiquated telephony (Shakarian, Shakarian, & Ruef, 2013). The term "smart grid" is currently being used to describe a variety of initiatives aimed at modernizing this communication infrastructure for better oversight, defense, and reliability (Easttom, 2018; Shakarian, Shakarian, & Ruef, 2013). But, like any other process comprising computer systems, cyber security ought to constitute a top priority, irrespective of whether the electric grid in issue is employing ancient or contemporary technology. In addition, many nations may see attacks on the electricity network as a preemptive strike owing to the importance of electricity in contemporary life, which is why we've included it in our discussion of cyberwarfare.

As was previously said, the purpose of a power grid is to link generators of electricity with those who use it. Transmission and distribution are the backbones of the grid. The term "transmission" refers to the process by which electricity is sent from the point of generating to intermediate substations that serve residential and commercial customers (Droege, 2012; Izycki & Vianna, 2021; ICRC, 2020; Shakarian, Shakarian, & Ruef, 2013). In most cases, high voltage

(100 kV or greater) is used throughout this part of the delivery (Shakarian, Shakarian, & Ruef, 2013). The part 2 is distributing, which is the transmission of electricity from substations to end users at a voltage of less than 100 kilovolts (Shakarian, Shakarian, & Ruef, 2013). The energy is transformed from high to medium or low energy by transformers at the substation.

Corporate, control center, and substation levels perform the primary duties of the electricity grid, respectively. The corporate level is responsible for business management and operational management (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). The control center is the hub of all real-time activities, including monitoring and forecasting. Substations are generally used for real-time monitoring of everyday activities (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). In each of these three stages, I.T systems are utilized in different ways. At the corporate level, IT platforms are depended upon for both asset management (predicting when specific substations may undergo repair, leading to a determination to divert energy from that substation (Izycki & Vianna, 2021)) and forecasting the quantity of energy that must be produced the next day (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). In order to control and monitor the electricity sent to the substations, the control level makes heavy use of automation systems including energy management systems (E.M.S), human-machine interfaces (H.M.Is), and a Front End Processor (F.E.P) (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). Last but not least, substations rely heavily on Technology for monitoring consumer energy distribution. At this tier, it is expected to find devices like programmable logic controllers (P.L.Cs) and remote terminal units (R.T.Us).

There are 3 primary types of cyber assaults on power grids: component-level, protocol-level, and topology-level (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). Component-wise assaults target isolated elements of the I.T systems that support the power grid. The Aurora

Test, in which a breaker switches were opened and shut in such a way as to force a power generator out of harmony with the rest of the electricity network, this is an instance of a component-wise assault (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). The preceding are some other instances of component-wise assaults, but are by no means exhaustive:

- Operations that intentionally provide a user false information (i.e., a violation of nonrepudiation)
- Attempted destruction of infrastructure vital to the distribution of electricity
- Operations aimed at disabling a component of the electrical grid

When someone conducts a protocol-wise assault, they try to disrupt the transmission protocol used to send data about the electrical system. Inter Control Center Protocol (I.C.C.P) and Distributed Networking Protocol (D.N.P) (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013) are 2 of the many non-standard communication protocols often used by electric grid control centers and substations. These protocols, nevertheless, are not entirely exclusive to devices used in electric energy automation (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). The D.N.P specification is available for a little price, as an instance. A “Man-in-the-Middle” cyber exploit is the most common protocol-based assault since it allows the hacker to alter communications among the target and the hacker. Possible outcomes of such an assault might include:

- The overproduction of electricity results in financial losses for energy providers
- Concerns about danger (that is to say, energizing a line when energy workforce are striving to mend it)
- Power surges can cause serious problems for your electronics and/or equipment

The cyberattack on “Maroochy Water Services” was mentioned before in this research serve as an example of a very basic protocol attack. Septic system pumping stations were compromised because a hacker exploited a weakness shared by all unprotected wireless communication schemes.

An initial step for the hacker is to get into a S.C.A.D.A. network used to keep tabs on or manipulate a subsystem of the energy grid (Eduardo Izycki, 2021; Shakarian, Shakarian, & Ruef, 2013). Breach to S.C.A.D.A systems is typically achieved through 1 of 3 channels: communication between the corporate network and S.C.A.D.A, over a virtual private network (V.P.N), or/and from a distant location (Izycki & Vianna, 2021; Shakarian, Shakarian, & Ruef, 2013). The corporate level frequently requires data generated by multiple S.C.A.D.A systems. Businesses often utilize S.Q.L (it could also be custom-built) databases (Izycki & Vianna, 2021; Shakarian, Shakarian, & Ruef, 2013), which S.C.A.D.A systems connect to and query via interfaces. The point at which information is sent from the S.C.A.D.A system to the database server is potentially vulnerable to a cyberattack. Gaining illegal accessibility to S.C.A.D.A systems also frequently occurs through the use of V.P.N connections (Radvanovsky et al., 2016; Shakarian, Shakarian, & Ruef, 2013). These connections are typically utilized as a part technical support or personnel's who need accessibility to S.C.A.D.A systems from the workplace, but can be hijacked if the client machine running the V.P.N software is compromised. Remote site communication is a 3rd accessibility mechanism (Radvanovsky et al., 2016). This occurs because of the need for trust among some electrical grid components that may not be in close proximity to one another. An entry point may be gained if the link of communication among 2 such systems was broken. Back-up centers, quality assurance networks, and electrical substations are all examples of off-site locations.

The cybercriminal has to know how the system works in order to carry out the hack successfully after they have gained entry to it. Assuming the hacker doesn't have access to any other intel, he / she will need to sift through data from the power-grid automation systems to figure out how the S.C.A.D.A system in question is built. The intricacy of S.C.A.D.A systems is 1 of the finest barriers against attack, requiring significant effort on the part of the attacker. The hacker may utilize active scanners, which has a high risk of being spotted by the cybersecurity administrator, or passively monitoring of traffic to and from a S.C.A.D.A system in order to determine the communications protocol in use.

If a cybercriminal has learned enough about a S.C.A.D.A system to manipulate it, they may launch a successful assault. As such, the hacker is likely to look for high-payoff targets (H.P.Ts) (Radvanovsky et al., 2016), or systems that, if compromised, would considerably increase the intruder's potential to obtain control. The S.C.A.D.A system communicates with the various process controllers via the Front End Processor (Radvanovsky et al., 2016; Zahra & Christianti, 2021) (or numerous F.E.Ps, as is sometimes the case). The F.E.P will be able to talk to any of these controllers, regardless of their protocol (Shakarian, Shakarian, & Ruef, 2013). So, the issue of decoding the procedures to each of the process controllers is sidestepped if the hacker has access to the F.E.P. Numerous instructions submitted to the F.E.P do not need to be authenticated or verified (Russell, 2014). Nevertheless, the F.E.P often does not keep a log of orders. As the hacker must transmit orders to the F.E.P, the attack is conducted at the protocol level. The Human Machine Interface is the second high-reward area (Radvanovsky et al., 2016; Shakarian, Shakarian, & Ruef, 2013) to be examine. Operators access the S.C.A.D.A system using the H.M.I, which is housed on a local workstation (Radvanovsky et al., 2016). So, it would be simpler for a hacker to decipher and alter if it were compromised. The H.M.I is an assault at the level of individual components, as opposed to the F.E.P's attack at the protocol level (Radvanovsky et al., 2016; Shakarian, Shakarian, & Ruef, 2013). Furthermore, since it is installed on a workstation, the hacker may be able to exploit common I.T-style weaknesses. Nonetheless, H.M.Is often include safeguards to prevent damage from being caused by human mistake. An intruder could also try to get into the Engineering Work Station (E.W.S), which is used for making things. It can seem like an H.M.I on the outside but have less cybersecurity measures on the inside.

The U.S. Department of Energy (D.O.E) orchestrated an experiment in 2007 called the "***Aurora Experiment***" (Kashimer, 2016; Clayborn, 2021; Shakarian, Shakarian, & Ruef, 2013) to ascertain if a legitimate cyber attack against a real-world generator would be feasible. This should not be confused with "Operation Aurora," the cyber attack aimed at theft of intellectual assets from Google and other major firms. Idaho National Laboratory of the D.O.E. conducted a test in 2007 in which a power generator was cyberattack remotely (Izycki & Vianna, 2021; Jarmakiewicz, Parobczak, & Maślanka, 2017; Kashimer, 2016; Cronin & Marion, 2016; Shakarian, Shakarian, & Ruef, 2013). The generator ran on fuel and produced 3.8 MV at 60% load (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). The conclusion was detailed in an unclassified footage sent by D.H.S (Department of Homeland Security) to the Associated Press (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). The generator begins to vibrate in the footage. A cataclysmic breakdown is shown after a few seconds of soot filling the display.

A generator's frequency, voltage, and phase rotation must all fall within a specific tolerance when it is linked to the network (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). If not, the connection will be prevented by protective relays. The limits for these variables might vary for brief periods of time to provide a steady electricity supply and prevent the early disengagement of generators. Short windows of opportunity like this were used to full effect in the Aurora Experiment. The goal of what has been dubbed the "Aurora assault" (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013) is to disrupt the generator's ability to keep in phase with the electrical grid for long enough to induce failure, without actually disconnecting the generator from the grid.

The Aurora flaw allows a hacker to toggle between opening and closing a breaker in a shorter time period than is permitted by the protective relays (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). There is a lot of strain on the generator, especially the shaft, when it is out of phase with the rest of the power system (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). The breaker opens, the generator experiences stress for a brief amount of time while out of rhythm with the grid, and the breaker shuts again, barely in time to prevent disconnection by the protective relay. In the long run, the shaft will break under the weight of all the tension that will have been applied to it. After 13 repetitions (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013), the Aurora Experiment generator started to tremble unnaturally. It took 22 cycles for soot to appear (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). The experiment performed by Idaho National Laboratories is instructive, but it raises the question of how likely it is that an assault of this sort could ever be carried out in the real world. Nevertheless, the assault is still conceivable if the attacker knows enough about the computer system and the energy plant to compromise both. Assailants might use a variety of tactics;

- As a physical assault, the enemy repeatedly opens and closes the breaker, preventing the power generator from functioning (Shakarian, Shakarian, & Ruef, 2013). Although though such a technique isn't particularly advanced, it may do significant damage to the equipment if it were repeatedly performed at irregular intervals.

- By infiltrating the communication corridor between the breaker and the outside world, an attacker can provide orders to the breaker. It is possible for a hacker to give the breaker directives to open and shut.
- This type of attack involves the cybercriminal connecting straight to a port on the protection relay, so evading any network security mechanisms that may otherwise keep anyone from corrupting the communications channel (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). Linking the generator to the network without first running the defense algorithm that checks the voltage, frequency, and phase rotation to make sure they are all within acceptable ranges is a possibility. This identical mechanism might be used by the hacker to take control of the breaker.
- Maybe the most sophisticated kind of assault is when a hacker installs malicious code directly into the protection relay itself. The hacker can directly control time or power levels by inserting coding into the relay's logic or operating system (Kashimer, 2016), perhaps in conjunction with other assaults. It would be simple for the hacker to overcome most security measures and generate false reports (in violation of non-repudiation) claiming that the relay is operating correctly if they were able to plant such a malware.

If one is developing defenses against an Aurora-style intrusion, one should take into account more than just the 4 hacker attacks listed previously. Certain generators, for contrast, might feature a "syncing check" that prevents breaker operation, unless generator and grid voltage and frequency are in synchronicity. This function of the generator was turned off during the Aurora Experiment. There are, nonetheless, certain circuit breakers that aren't physically connected to the power source. If a breaker at a tie-in points other than the generator was to be attacked in an Aurora-style operation, the synchrony verification would not occur.

In anticipation of launching an Aurora-style cyberattack, an adversary must first defeat certain security protocols (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013). They classify these defenses into 3 broad categories (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013), all of which contribute to the system's cyber security. Standard cybersecurity concerns, such as authentication, encrypted communications, etc., must be surmounted, and a hacker has to know the computer network the generator is connected to (Radvanovsky et al., 2016). Given that an attacker may try to impede the synchrony of the power generator and the grid by opening and shutting the relay or gaining access to the protective dispatch, safeguarding these breakers is critical (as demonstrated by the Aurora Test). The hacker ought to be capable of unlocking and closing the breaker in such a way that the protection relay does not trip, or else the generator will be cut off (either by precise timing or by sabotaging the protective relay). Last but not least, the attacker needs precise information about the target system. In order to create system failure by breaker manipulation, for example, the attacker has to know that the breaker may undergo several re-closes and/or cycles of open/close events before any harm is done (Kashimer, 2016; Shakarian, Shakarian, & Ruef, 2013).

Although the Aurora Experiment was only an experiment, it showed that a cyber assault may have real-world consequences. In addition, the experiment stimulated vital investigation into ways to lessen the impact of cyberattacks on the electrical infrastructure. The Aurora Experiment is a form of cyber assault on a single piece of industrial machinery, similar to those detailed earlier in this study.

This does not mean, nonetheless, that assaults based on the topology of power-grid networks are irrelevant or impossible. Although there have been no documented instances of cyber assaults leading to such debacles, several scholarly publications have shown that it is conceivable to do so (Kashimer, 2016; Clayborn, 2021; Shakarian, Shakarian, & Ruef, 2013). Numerous real-world infrastructure networks are highly improbable to fracture in the presence of random failures, as was previously established in this research. This is because the amount of electrical lines connecting any specific energy plant to the network varies significantly. Nevertheless, the network's vulnerability to random failure increases dramatically when humans are included in the possibility of cascade failure due to dependency on another network (namely, the network of Internet routers). This makes it more likely that adversaries will be able to breach communication-dependent parts of the energy grid.

Findings & Recommendations

Several forms of technology and varying from technological advancements are vulnerable to attacks by many states and non-state players in different ways, as shown by these case studies throughout this study. In order to analyze the research questions for this study and provide a conclusive verdict, the analysis will provide the findings as a whole verdict and separate what is common across all cases provided throughout this study, that is; recognizing cyber ordnance and the pertinency to apply I.H.L. The study proves successful by corroborating that International Humanitarian Laws are applicable to “Cyberwarfare”; its demonstration shows that contemporary Cyber Spectrum evolution can operate as a solitary/single weapon affecting the prospect for human loss of life or critical infrastructure impair/destruction or the equivalent of an act of aggression. The study findings shows that despite the fact that I.H.L is relevant to cyber warfare, its purview is quite constrained, as the existing I.H.L framework only necessitates a legal examination of such armaments and demands for these 'new means and ways of warfare' to be compliant with the norms of I.H.L.

Joining the more conventional "ground," "water," "air," and "spatial" spectrum, A "5th" spectrum of warfare has emerged as the armed–forces increasingly rely on information and communication technologies. Operations using digital infrastructure have become increasingly common, with both state and non-state actors resorting to more sophisticated methods in recent years. There is a pressing need to investigate how international law regulates cyber warfare because it is a relatively new realm where assaults are being undertaken. The Tallinn Manual is a non-binding publication that analyzes the utilization of I.H.L to cyber procedures/ops (Zahra & Christianti, 2021), however there is currently no treaty that deals directly with the creation and deployment of cyberwar. Nonetheless, more clarity is needed on a number of issues within the intended legislative framework, and this may potentially take the shape of future state practice in this sector.

Existing international norms concerning the use of force do not prohibit cyber weapons in the same manner as they prohibit certain types of conventional, biological, and chemical weapons. Nonetheless, Article 36 of Additional Protocol I to the Geneva Conventions (ICRC, 2020) suggests that I.H.L is a flexible legal framework that may be interpreted in a variety of contexts. This section, commonly referred as the "armaments/weapon review" clause, mandates that nations examine whether or not the deployment of a novel weaponry, means, or tactic of conflict violates international law. Article 36 emphasizes that I.H.L. applies to more than only armaments that existed at the time these rules were drafted (ICJ, 2023). Hence, even if a specific technology isn't mentioned in the statutes, the regime still applies because it is a general obligation. By signing I.H.L. accords, governments accept that they will govern any disputes between them in the future. This view is supported by the International Court of Justice's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, in which the court stated that "all forms of warfare and to all kinds of weapons, including those of the future," (ICJ, 2023; ICRC, 2020) fall under the purview of I.H.L's rules and principles. As "cyber weapons" are a novel means and tactic of warfare, nations must first confirm that they are in conformity with I.H.L before employing them in combat.

I.H.L. is a framework that imposes responsibilities and provides safeguards on parties to armed conflicts, making it crucial to determine whether or not this applies to cyber activities. Cyber activities only fall under the jurisdiction of I.H.L. if they take place during or in relation to an actual or threatened military confrontation. These wars can either be considered intercontinental or non-intercontinental. It is important to evaluate the criteria essential for each kind of warfare to decide which law applies within I.H.L. Cyberwarfare provide unique difficulties in distinguishing between intercontinental and non-intercontinental armed conflict status for the purposes of I.H.L.

The use of aggression amongst nations, no regardless of how minor or severe, would result in the adoption of I.H.L. In addition, there is no predetermined legal framework for the use of action, thus cyber activities or a hybrid of cyber and kinetic activities may be used in warfare amongst nations. The problem emerges when actions by non-state players or private persons may be traced back to a certain province, thereby elevating the confrontation to a global scale. In pursuit of preventing direct accountability, nations will often use private organizations to carry out cyber activities. In these cases, it is essential to prove the Nation's efficient management over the cyber activity. As this would constitute an act of intercontinental warfare if 2 or more Countries with effective authority over such bodies were engaged, the rights and responsibilities guaranteed by the Geneva Conventions would apply. The origin of the attackers or the computer used to initiate the assault might be in a different jurisdiction, posing challenges when trying to assign liability and establish authority in the virtual realm.

While though the principles of I.H.L. pertain to its kinetic and cyber activities, it might not always be obvious how these standards may extend to cyberwarfare because they were designed with procedures in perspective. In light of this research, two conclusions may be drawn. Physical characteristics are the only ones that may be used to define an "object," hence only things that can be observed and handled are eligible. There needs to be a physical effect and/or a degradation of capability of the targeted system or network for the norms of I.H.L to apply to cyber warfare. Yet, data may be thought of as an "object" because it can be physically assaulted and destroyed. Thus, it may be a breach of the principle of distinction when nations or non-state players hack into vital civilian data such as medical records, biometric information, bank account information, it's possible that doing so would go counter to the principle of differentiation.

Classifying civilian data as a 'noncombatant object' is another important problem when trying to differentiate amongst civilian objects and military goals. Although civilian assets and military targets have been defined in the L.o.A.C, it is not clear whether 'civilian data' such as medical records, biometric information, etc. would be deemed a 'noncombatant object' in the context of cyber operations. Data is not often viewed as an "item" in the traditional sense. The Tallinn Guide arrived to this result by considering information to be 'intangible,' and so distinct from 'object,' thus the conventional sense (Zahra & Christianti, 2021). Yet, the disruption of the other country's cyber systems critical infrastructure due to data targeting would still be considered an assault.

As cyber attacks become more common, it will be crucial to establish the point at which they become disproportionately harmful to innocent citizens. An easy way to think of proportionality is as a limit on aggression. As a result, it is crucial to use proportionality while initiating cyber warfare to make sure the assault doesn't go beyond the bounds of I.H.L.

The Tallinn Manual asserts that the proportionality principle can be used to cyber operations (Zahra & Christianti, 2021). Cyber activities are covered by the L.o.A.C, according to the Tallinn Manual (Zahra & Christianti, 2021); this means that the principle of proportionality must also be upheld. These days, it's not uncommon to find technology that serves more than one purpose; some systems, for example, can be used for both armed services and civilian purposes. Systems like these include energy plants that provide electricity to both noncombatant and armed services locations and critical infrastructure systems that serve civilian and military facilities. Proportionality analysis in cyber warfare would necessitate a differentiation between dual-systems. Albeit, the noncombatant employment of dual-use technologies challenges the implementation of the proportionality rules, even though such assets can be classified as military objectives. Collateral harm is likely to occur if dual-systems are attacked.

The concept of the indirect implications that flow from the direct results of a specific action, remains a challenge when applying proportionality throughout cyber operations. Cyberspace is so vast that it's hard to predict how an attack on one part of the internet will influence other parts of the internet, or how far its effects will spread. Also, the interrelated nature of cyber systems makes it harder to foretell any particular ripple impact.

In contrast to physical combat, where violators may be easily identified, this is not the case in cyber domain. With the furtherance of proxies and other anonymizing technologies, nowadays it's exceedingly inconceivable to pinpoint cybercrime on any one particular country. Attributing cyberwarfare is essential for holding players responsible for I.H.L breaches. Nations are liable for their actions that can be directly linked to them pursuant to international law. The Nation will be found liable under the I.H.L for its role in the following instances where responsibility lies with it:

- Governmental entities;
- Individuals or groups subject to the Nation's control;
- people or organizations operating beneath governmental authority;
- Individuals or organizations whose actions the government officially endorses.

Hence, a country would be responsible for any infringements of intercontinental statute committed by cyber operations undertaken by governmental agencies, private corporations, or individuals whose action the country endorses as its own or upon whom the nation exerts its influence or authority. Unfortunately, this strategy faces significant obstacles. Since cybercriminals often go to great lengths to conceal their origins and orchestrate their operations, it can be next to impossible to determine who is actually responsible for a cyberattack. As a result, pinning responsibility for cyber assaults on one province on another gets exceedingly challenging. It might, therefore, be feasible to figure out who is behind the assault if there is proof of the location of the system used to initiate it or if human intelligence can deduce who is behind it. Hence, there could be specific cases when identification is feasible.

As expounded upon in this present study a recommendation is drawn-up upon this study; I.H.L is relevant to novel modes and techniques of warfare, thereby rendering these regulations pertinent to cyber warfare in the context of both International Armed Conflict and non-International Armed Conflict. Adherence to the legal framework governing armed conflict necessitates observance of the three fundamental principles of I.H.L, namely distinction, proportionality, and precautionary measures during a war of aggression. The absence of sophisticated technologies whilst the formulation of the L.o.A.C necessitates the introduction of new laws that specifically address cyber warfare. This is due to the challenges that arise in applying the three fundamental principles of I.H.L during cyber operations.

The applicability of I.H.L to cyber warfare is constrained by its narrow scope. The existing I.H.L framework mandates solely the legal assessment of cyber weaponry and necessitates compliance with the three fundamental principles of I.H.L, namely distinction, proportionality, and precautions in assault, in relation to these "new means and techniques of hostilities”. However, the law does not address other aspects, such as the attribution of cyber attacks. Furthermore, the existing legal framework governing armed conflicts provides safeguards for safeguarding civilians and civilian property from acts of violence, yet its applicability in the context of cyber operations remains uncertain. This is due to the intricate interdependence between armed forces and non-military cyber infrastructure, which poses significant challenges in extending security to civilians’ cyber infrastructure. Consequently, it is imperative to introduce a specialized agreement that comprehensively addresses cyber warfare, with a particular emphasis on the Tallinn Manual's discoveries concerning the examination and relevance of I.H.L to cyber warfare, with the aim of enhancing cybersecurity.

In addition, it is imperative to address the restricted scope of the principle of proportionality in the context of cyber operations. To mitigate the potential for severe cyber repercussions, it is essential to establish a standardized proportionality criterion within a comprehensive global agreement that all parties involved in a cyber operation must adhere to. It is imperative for military entities to perform a proportionality assessment prior to engaging in any cyber-attack that has the potential to result in unintended harm to non-combatants or civilian infrastructure. To further ensure the safety of citizens and civilian infrastructure, forces undertaking cyber operations must adhere to the 'continuous care norm' outlined in the Additional Protocol I, even if such actions are not classified as assaults. It is advisable for military organizations to seek the counsel of cyber specialists in order to comprehend the potential ramifications of their attacks or operations on a given system. This will aid in assessing the potential degree of harm that may occur as an incidental consequence to the lives of non-combatants or civilian infrastructure. In addition, it is recommended that countries implement preventative measures such as establishing alert systems for detecting cyber attacks, conducting training for civil defense personnel, and monitoring networks to differentiate amongst civilian and military targets in the context of cyber operations.

Conclusion

Many of the most notable cases of cyberwarfare from the past few years were investigated in this study/report. Until recently (at the time of writing this research), there was speculation about cyberwarfare but little evidence (at least in the public sphere) that it had transpired. Some even contended that cyberwarfare wouldn't ever be a real danger. Since then, developments and cyber operations such as the Russia-Georgia war of 2008, Chinese Cyber Warfare, The Hezbollah 2006 July War, too Weaponizing Cyber Tools Upon Critical Infrastructure, and developing cyber concerns in contemporary and future time, seem to have altered the argument on cyber warfare from " Do we put any importance on the cyber war?" to "What ought to be done regarding cyber warfare?" and "Can the contemporary International Laws apply to cyber warfare?". In this study, the upshot became known that a multitude of the operations predicted in the 1990s actually occurred in the early & late 2000s. The study analyzed at how the cyber spectrum helps with physical operations on the ground as well as how governments utilize the cyber spectrum as a propaganda weapon or to suppress internal discontent. Although, nation-states and formal institutions aren't the only ones using the Internet for political purposes.

This research also provides a peek of the effects of expanding global, border-crossing online social networks. Although it has gained prominence in the last several years, it is simply the amplification of the global citizen, who is now more empowered than ever to express his/her dissatisfaction with issues far removed from his/her actual home base. Lawbreaker and, to a lesser degree, politicized biased travesties of social networks draw attention to the intrinsic hazard of global interconnection, which is regrettably only incrementally permeating the corpus of general/common sense.

Some sections of this study not only detail past case studies, but also squeeze attention to the potential outcomes arising from the further development of cyber spectrum. Many researchers, including this current study, have attempted to extrapolate from current scientific and technological trends in order to foresight feasible hypothetical future of cyber warfare strategies. Cyberspace will nonetheless develop into a multi-dimensional battleground. Cybersecurity is entering an entirely novel phase, one that will likely undergo significant transformations before stabilizing, – that is assuming stabilization is even feasible.

Impending the endgame, we are. But this is the endgame of orthodox warfare. Choose mankind must, how to retort to their foresight. But memorize always, in motion is the future, multitudinous conceivable futures there are.

Determine to grasp the one secret of victorious warfare. No longer certain that one ever does win a war, I am. For in warfare, we have, the destruction of life already lost.

Yet, attainable to us, a route whose destination is mysterious to us. Seeking the route of victory, yet to uncover we are. Not victory in the International Laws, Cyberspace, warfare; but victory of all times, – peace and human unity.

References

Adonis, A. A. (2020, Mar). *International Law on Cyber Security in the Age of Digital Sovereignty*. Retrieved from E-International Relations: https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

Altamura, J. M. (2020). *Chinese Malware: Historical Perspective of Tactics and Methodologies Utilized to Steal Intellectual Property and Data*. Retrieved from ProQuest: https://www.proquest.com/docview/2476123966?parentSessionId=FBfhrp2o8siKdA%2B18QWGQk5l%2Ff9AEO6AQUSN6f7finM%3D&pq-origsite=primo&accountid=27203

Boulanin, V., Bruun, L., & Goussac, N. (2021, Jun). *Autonomous Weapon Systems and International*. Retrieved from sipri: https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf

Brenner, J. (2011). *America the Vulnerable.* The Penguin Press.

Buchan, R. (2016). *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*. Retrieved from HeinOnline: https://heinonline-org.ezproxy.libproxy.db.erau.edu/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/chnint15&men_hide=false&men_tab=toc&kind=&page=741#

Buresh, D. L. (2021, Aug). *Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects*. Retrieved from openaccesspub: https://openaccesspub.org/jafs/article/1686

Clayborn, M. (2021). *Cyberwarfare: Defining the Threshold*. Retrieved from ProQuest: https://www.proquest.com/docview/2557180271/fulltextPDF/5AC586C7E8E74932PQ/1?accountid=27203

Cohen, M. S., Freilich, C. D., & Siboni, G. (2016). *Israel and Cyberspace: Unique Threat and Response*. Retrieved from JSTOR: https://www-jstor-org.ezproxy.libproxy.db.erau.edu/stable/26393471?searchText=Cyberwar+Taking+stock+of+security+and+warfare+in+the+digital+age&searchUri=%2Faction%2FdoBasicSearch%3Fscope%3DeyJwYWdlTmFtZSI6ICJJbnRlcm5hdGlvbmFsIFN0dWRpZXMgUGVyc3BlY3RpdmVzIi

Colarik, A., & Janczewski, L. (2012, Apr). *Establishing Cyber Warfare Doctrine*. Retrieved from Journal of strategic security: https://scholarcommons.usf.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1123&context=jss

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed.* SAGE Publications, Inc.

Cronin, K., & Marion, N. E. (2016, Dec). *Critical Infrastructure Protection, Risk Management, and Resilience*. Retrieved from Taylor & Francis: https://www-taylorfrancis-com.ezproxy.libproxy.db.erau.edu/books/mono/10.1201/9781315310657/critical-infrastructure-protection-risk-management-resilience-nancy-marion-kelley-cronin

Deibert, R. J. (2018). *Toward a Human-Centric Approach to Cybersecurity*. Retrieved from ProQuest: https://www.proquest.com/docview/2151891130?parentSessionId=G%2BSJMQyeMVSZmHTePJTjjnKc4JL8Eqr8KQw%2F6VNAIaI%3D&pq-origsite=summon&accountid=27203

Droege, C. (2012, Jun). *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*. Retrieved from ProQuest: https://www.proquest.com/docview/1370609087/fulltextPDF/AE58F349254E43CAPQ/1?accountid=27203

Dunlap, C. J. (2011). *Perspectives for Cyber Strategists on Law for Cyberwar*. Retrieved from ProQuest: https://www.proquest.com/docview/857934309/fulltextPDF/42266C13CE1D4E3FPQ/1?accountid=27203

Dwyer, C. (2018). *Israel Acknowledges Having Bombed A Suspected Syrian Nuclear Reactor In 2007*. Retrieved from NPR: https://www.npr.org/sections/thetwo-way/2018/03/21/595727058/israel-acknowledges-having-bombed-a-suspected-syrian-nuclear-reactor-in-2007

Easttom, C. (2018). *The Role of Weaponized Malware in Cyber Conflict and Espionage*. Retrieved from ProQuest: https://www.proquest.com/docview/2018927237/fulltextPDF/DFFEB835EEDA4FC6PQ/1?accountid=27203

Eichensehr, K. E. (2015). *Cyberwar & international law step zero*. Retrieved from Nexis Uni: https://advance-lexis-com.ezproxy.libproxy.db.erau.edu/document/?pdmfid=1516831&crid=dda11732-f48f-44c8-b3d1-c5cbf9a39774&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5GNX-CNK0-00CV-9154-00000-00&pdcontentcomponentid=146

Eun, Y.-S., & Aßmann, J. S. (2016). *Cyberwar: Taking Stock of Security and Warfare in the Digital Age*. Retrieved from JSTOR: https://www-jstor-org.ezproxy.libproxy.db.erau.edu/stable/26393473

Evans, D. G. (2018). *The evolution of electronic warfare: a timeline*. Retrieved from Army Technology: https://www.army-technology.com/features/evolution-electronic-warfare-timeline/

Faga, H. P. (2017, Apr). *The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century*. Retrieved from ProQuest: https://www.proquest.com/docview/1961535654?parentSessionId=%2BtkyZyxL0lq4qaUCNQEeqRzPG11aXpHRKQlcpixKggU%3D&pq-origsite=primo&accountid=27203

Farwell, J. P., & Rohozinski, R. (2011, Jan). *Stuxnet and the Future of Cyber War*. Retrieved from Taylor & Francis Online: https://www-tandfonline-com.ezproxy.libproxy.db.erau.edu/doi/full/10.1080/00396338.2011.555586

Gable, K. A. (2010). *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*. Retrieved from Hein Online: https://heinonline-org.ezproxy.libproxy.db.erau.edu/HOL/Page?collection=journals&handle=hein.journals/vantl43&id=59&men_tab=srchresults#

Gisel, L., Rodenhauser, T., & Dormann, K. (2020, Apr). *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*. Retrieved from ProQuest:

https://www.proquest.com/docview/2501950609/fulltextPDF/ED4B456946D24B7EPQ/1?accountid=27203

ICJ. (2023). *ICJ, Nuclear Weapons Advisory Opinion*. Retrieved from How does law protect in war?: https://casebook.icrc.org/case-study/icj-nuclear-weapons-advisory-opinion

ICRC. (2020, Nov). *International Humanitarian Law and Cyber Operations during Armed Conflicts*. Retrieved from ICRC: file:///C:/Users/Shawn/AppData/Local/Temp/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

Izycki, E., & Vianna, E. W. (2021, Feb). *Critical Infrastructure: A Battlefield for Cyber Warfare?* Retrieved from ProQuest: https://www.proquest.com/docview/2505730222/fulltextPDF/63D64BC2722A4469PQ/1?accountid=27203

Japaridze, T. (2020, Oct). *No more complacency: A robust cybersecurity strategy for Georgia is overdue*. Retrieved from European Leadership Network: https://www.europeanleadershipnetwork.org/commentary/no-more-complacency-a-robust-cybersecurity-strategy-for-georgia-is-overdue/

Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017, Jul). *Cybersecurity protection for power grid control infrastructures*. Retrieved from ScienceDirect: https://www-sciencedirect-com.ezproxy.libproxy.db.erau.edu/science/article/pii/S1874548216300324

Karatas, S. S. (2022, Jan). *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance*. Retrieved from SpringerLink: https://link-springer-com.ezproxy.libproxy.db.erau.edu/article/10.1365/s43439-021-00045-4#Sec12

Kashimer, D. (2016). *Industrial control systems in the energy sector*. Retrieved from ProQuest: https://www.proquest.com/docview/1839342749?accountid=27203&parentSessionId=BSa1Z1EjscjPTbM9bYETRqd60ehhYRnPJfCi9MymMGQ%3D&pq-origsite=primo

Kelly, B. B. (2012, Oct). *Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*. Retrieved from ProQuest: https://www.proquest.com/pagepdf/1328333278/fulltextPDF/71A5A2CABA1547D5PQ/1?accountid=27203

Koblentz, G. D., & Mazanec, B. M. (2013, Nov). *Viral Warfare: The Security Implications of Cyber and Biological Weapons*. Retrieved from Taylor & Francis Online: https://www-tandfonline-com.ezproxy.libproxy.db.erau.edu/doi/full/10.1080/01495933.2013.821845

Kovacs, L. (2018). *Cyber Security Policy and Strategy in the European Union and NATO*. Retrieved from sciendo: https://sciendo.com/article/10.2478/raft-2018-0002

Lewis, J. A. (2002, Dec). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Retrieved from ResearchGate: https://www.researchgate.net/profile/James-Lewis-9/publication/245508226_Assessing_the_Risks_of_Cyber_Terrorism_Cyber_War_and_Other_Cyber_Threats/links/5e25be2192851c89c9b49515/Assessing-the-Risks-of-Cyber-Terrorism-Cyber-War-and-Other-Cyber-Threats.pdf

Liaropoulos, A. (2015). *A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia*. Retrieved from JSTOR: https://www-jstor-org.ezproxy.libproxy.db.erau.edu/stable/pdf/26487503.pdf?refreqid=excelsior%3A3abbaddc4398c04112a30f552c043500&ab_segments=&origin=

Liles, S. (2012). *Cyber warfare as a form of conflict: Evaluation of models of cyber conflict as a prototype to conceptual analysis(Dissertations)*. Retrieved from ProQuest: https://www.proquest.com/docview/1238278265?parentSessionId=e18dkmP%2BTJsmpsalXNkNvJo%2BKv1G9eLzsWuZubkCmD8%3D&pq-origsite=primo&accountid=27203

Marsili, M. (2019). *The War on Cyberterrorism*. Retrieved from Taylor & Francis Group: https://www-tandfonline-com.ezproxy.libproxy.db.erau.edu/doi/epdf/10.1080/17419166.2018.1496826?needAccess=true&role=button

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). *Cyberoperations and International Humanitarian Law*. Retrieved from ProQuest: https://www.proquest.com/docview/2093306070/fulltextPDF/37C894F84C404503PQ/1?accountid=27203

Poirier, W. J., & James Lotspeich. (2013). *Air Force Cyber Warfare: Now and the Future*. Retrieved from Defense Technical Information Center: https://apps.dtic.mil/sti/citations/ADA589641

Prescott, J. (2011, Dec). *War by Analogy US Cyberspace Strategy and International Humanitarian Law*. Retrieved from Taylor & Francis Online: https://www-tandfonline-com.ezproxy.libproxy.db.erau.edu/doi/full/10.1080/03071847.2011.642683

Pyzynski Mariusz, B. T. (2021, Jun). *Cybersecurity of the Unmanned Aircraft System (UAS)*. Retrieved from ProQuest: https://www.proquest.com/docview/2528311402?parentSessionId=6WBdqIKGS29rZN50jtrj5Q66UHLJAsamkkUNi5orklA%3D&pq-origsite=primo&accountid=27203

Radvanovsky, R., Look, B. G., & Brodsky, J. (2016). *Handbook of SCADA/Control Systems Security*. CRC Press.

Rid, T. (2011, Oct). *Cyber War Will Not Take Place*. Retrieved from Taylor & Francis online: https://www-tandfonline-com.ezproxy.libproxy.db.erau.edu/doi/full/10.1080/01402390.2011.608939

Roscini, M. (2019). *Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes*. Retrieved from SpringerLink: https://link.springer.com/article/10.1007/s10609-019-09370-0#change-history

Roszak, P., & Horvat, S. (2022). *Religious Freedom, Cybersecurity, and the Stability of Society: Problems and Perspectives from a European Perspective*. Retrieved from ProQuest: https://www.proquest.com/docview/2679825675/fulltextPDF/CE7F34F2C2B448D0PQ/1?accountid=27203

Russell, A. L. (2014, Nov). *Cyber Blockade*. Retrieved from ProQuest: https://ebookcentral.proquest.com/lib/erau/detail.action?docID=1810129&pq-origsite=primo

Sanders, C. M. (2018). *The battlefield of tomorrow, today: Can a cyberattack ever rise to an "act of*. Retrieved from HeinOnline: https://heinonline-org.ezproxy.libproxy.db.erau.edu/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/utahlr2018&men_hide=false&men_tab=toc&kind=&page=503

Sandvik, K. B. (2015, Nov). *The humanitarian cyberspace: shrinking space or an expanding frontier?* Retrieved from Taylor & Francis Online: https://www-tandfonline-com.ezproxy.libproxy.db.erau.edu/doi/full/10.1080/01436597.2015.1043992

Saxon, D. (2016, Oct). *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions*. Retrieved from JSTOR: https://www-jstor-org.ezproxy.libproxy.db.erau.edu/stable/pdf/26298216.pdf?refreqid=excelsior%3Adfda20f62c1bc499f55f1dd5a6b5bf5d&ab_segments=&origin=&acceptTC=1

Schmitt, M. N. (2018, May). *Grey Zones in the International Law of Cyberspace*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687

Schmitt, M. N., & Watts, S. (2015). *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*. Retrieved from ProQuest: https://www.proquest.com/docview/1704865201/fulltext/83E6762BA8A44B94PQ/1?accountid=27203

Shackelford, S. J. (2017). *The Law of Cyber Peace*. Retrieved from ProQuest: https://www.proquest.com/docview/1991567004/fulltextPDF/7981C4B7B8C74A13PQ/1?accountid=27203

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare: A Multidisciplinary Approach.* Elsevier.

Sobelman, D. (2016). *Learning to Deter: Deterrence Failure and Success in the Israel-Hezbollah Conflict, 2006–16*. Retrieved from JSTOR: https://www-jstor-org.ezproxy.libproxy.db.erau.edu/stable/26777793?sid=primo

Sohail, H. (2022). *Fault Lines in The Application of International Humanitarian Law to Cyberwarfare*. Retrieved from ProQuest: https://www.proquest.com/docview/2661588237/fulltextPDF/5E5CBC416DA740B4PQ/1?accountid=27203&forcedol=true&parentSessionId=9C6rHf9wxVXaArjYme1XN76FpJ80KOgANf%2BySPv8pLk%3D&parentSessionId=kUl%2FZMWrJF%2Fy0cC6fp9wAaY47fzgi3f7WmjTqaO9hQo%3D

Stitilis, D., Pakutinskas, P., & Malinauskaite, I. (2017, Oct). *EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis*. Retrieved from ProQuest: https://www.proquest.com/docview/1957735344?accountid=27203&parentSessionId=lF07RExBEeCnb9NFsRX%2Ft0i9TrpoTJvN0uG7X3h%2FfMs%3D&pq-origsite=primo

Stockburger, P. Z. (2018). *From grey zone to customary international law: How adopting the precautionary principle may help crystallize the due diligence principle in cyberspace*. Retrieved from IEEE Xplore: https://ieeexplore-ieee-org.ezproxy.libproxy.db.erau.edu/document/8405020

Trinkunas, H., & Wallace, I. (2015, Jul). *Converging on the future of global Internet governance*. Retrieved from ProQuest: https://www.proquest.com/docview/1787813356?parentSessionId=zubCGsFqYac%2FaZDHfWxfMWFB9zZEEpwF5ewYRbzxxNQ%3D&pq-origsite=primo&accountid=27203

Voitașec, D.-I. (2015). *Applying International Humanitarian Law to Cyber-Attacks*. Retrieved from ProQuest:

https://www.proquest.com/docview/1748566203?parentSessionId=3mOe8DRB82f%2B1xHm6YP21DDpiam2feQgcrKTU3a04NU%3D&pq-origsite=primo&accountid=27203

Wallace, D. (2018). *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis*. Retrieved from CCDCOE: https://ccdcoe.org/uploads/2018/10/TP-11_2018.pdf

Zahra, I., & Christianti, D. W. (2021). *The Beginning of The International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual 1.0*. Retrieved from Padjadjaran Journal of International Law: http://jurnal.fh.unpad.ac.id/index.php/pjil/article/view/366

Zahra, I., Handayani, I., & Christianti, D. W. (2021, Feb). *Cyber-Attack in Estonia: a New Challenge in The Applicability of International Humanitarian Law*. Retrieved from Yustisia Jurnal Hukum: https://jurnal.uns.ac.id/yustisia/article/view/48336/31170