Universiteit Leiden
Institute of Security and Global Affairs

Master Thesis

Crisis and Security Management

The Principle of Proportionality in Military Cyber Operations

Name: Célestine de Zeeuw

Student number: s1542559

Email address: ccdzeeuw@gmail.com

Thesis Supervisor: Dr. Els de Busser

Second reader: Dr. Tatiana Tropina

Date: 12 January 2020

Preface

I would like to express my gratitude towards my thesis supervisor Dr. Els de Busser for her expertise and guidance in the past months. Especially for our enjoyable conversations about the future of cyber operations which provided valuable input to my research and further encouraged my interest on the topic. With this thesis my time as a student has come to an end and therefore, I want to express my appreciation to my unconditionally supportive family, friends and boyfriend who made these years very memorable.

Abstract

With the advent of rapidly developing technologies, nation states rely on their digital infrastructure in order to provide vital government services such as healthcare, energy and law enforcement. Consequently, the cyber domain appears to play a more visible role in military operations. IT networks have become an additional sphere of vulnerability where malicious state- and non-state actors are able to attack and damage critical infrastructures. The use of new technologies of warfare, has great impact on how civilians should be protected against the effects of hostilities. Although cyber attacks might be directed at computer systems rather than human beings, such operations could potentially cause severe human suffering. The Just War theory specifies ethical constraints with the objective to prevent unjust wars and the unjust conduct of wars, including the principle of proportionality. This principle seeks to limit the damage caused by military operations and requires that the effects of the means and methods of warfare must not be disproportionate to the anticipated military advantage sought. The principle of proportionality is legally set as limitation of warfare in international humanitarian law (IHL), which is rooted in traditional kinetic conflict. Due to the non-kinetic nature of cyber weapons, the applicability of traditional war regulations to cyber operations is not supposedly straightforward. In order to shed some light on the application of IHL to the context of cyber warfare, this thesis will place specific emphasis on how civilians are protected from the effects of military cyber operations by the principle of proportionality.

Keywords: Just War theory, cyber warfare, cyber, operations, international humanitarian law, the principle of proportionality, Stuxnet, Israeli Defense Force, Hamas

List of Acronyms

AIVD	Algemene Inlichtingen en Veiligheidsdienst (The Dutch General Intelligence and Security Service)
AP I	Additional Protocol I
HCJ	Israeli High Court of Justice
IAEA	International Atomic Energy Agency
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for the former Yugoslavia
IDF	Israeli Defense Force
IHL	International Humanitarian Law
IoT	Internet of Things
NPT	Nuclear Non-proliferation Treaty
UN GGE	United Nations Group of Governmental Experts

Table of Contents

Introduction

History tells us that every civilization has waged battles, which were characterized as barbaric and hardly limited by rules in the early ages. Nevertheless, from antiquity to modern society, civilizations have tried to impose certain limits on the use of violence in order to protect human security. In this respect, an institutionalized form of violence has derived which is today known as 'war' (Kolb & Hyde, 2008, p.38). Although developing regulations on warfare has been a universal concern throughout early history, it was not until the nineteenth century that the laws of war were codified in public international law. In 1859, a turning point occurred when the armies of tree countries clashed in the Battle of Solferino, Italy. This battle led to more than forty thousand deadly injured combatants who were left behind, without any medical assistance. Henry Dunant, a businessman from Geneva, observed this lack of respect for humanitarian values. Dunant publicized a book with a proposal "to protect and aid wounded and sick military personnel without adverse discrimination based upon nationality" (Kolb & Hyde, 2008, p.38). After strong incentives of lobbying, a committee named 'Geneva Committee' succeeded in persuading the Swiss government in order to adopt an international convention based on the proposals of Dunant, which are currently known as the Geneva Convention of 1864 (Kolb & Hyde, 2008).

This convention established the foundation of modern International Humanitarian Law (IHL). The legal framework of IHL aims to protect the civilian population from the effects of military operations. A critical point in the history of IHL has been the development of World War II (Kolb & Hyde, 2008, p.39). The horrors of this period led to a shift in the assumptions underlying in IHL. Before the Second World War, the IHL framework tended to concentrate particularly on military matters, along with administrative duties in occupied domains. A new way of thinking was adopted after the Second World War, where fundamental individual rights of civilians, both inside and outside occupied territory, were horrifically violated. Consequently, the fourth Geneva Convention was conducted against the backdrop of the Second World War, which gave new impetus to the role of IHL to protect certain persons that are not taking part in the hostilities from the evils of the war (Kolb & Hyde, 2008, p.40). It can be said that the legal framework of IHL, is continuously seeking an equilibrium point between two fundamental principles, which are the principle of humanity and the principle of military necessity. Both are crucial in order to regulate the fact that war possesses a certain hostile nature which cannot be ignored and on the other hand, the cruelty of war should be mitigated by regulations that institute the aim of controlling warfare (Kolb & Hyde, 2008). In this regard, a

strong rule of law ought to provide the protection of humanitarian rights and aims to mitigate violent conflict by providing legitimate processes for the resolution and regulation of hostilities.

As the law applied on armed conflicts has been continuously subject to change throughout history, the 21st century has posed unique challenges on the fundamental principles and the application of IHL. The reason for current challenges can be found in the development of cyberspace as the novel fifth domain of warfare in addition to the domains of land, air, sea and space. The use of cyber operations during armed conflict has come into reality. The development of technological innovation and the use of electronics and telecommunications in conflicts have expanded the battle space and introduced new ways to gain advantage over opponents (Robinson et al., 2017, p.1). States already publicly acknowledged that they have been using cyber operations during armed conflicts and the number of states developing cyber capabilities is ever increasing (ICRC, 2018, p.8). The new cyber domain of warfare is man-made and depends on electromagnetic networks composed of computers, cables and telecommunication components (Kasapoglu, 2017, p.2). The era of technology is generating sophisticated and complex means and methods of warfare that potentially can damage state's entire critical technological infrastructure.

Similarly, society's daily lives are controlled by technology to an unprecedented level. Water supplies, electricity generation, communication technology and health care systems of our globalized and technological interconnected world, make society increasingly vulnerable to attacks and other cyber operations during armed conflicts (Ayalew, 2015, p.210). Hostile actors can sophisticatedly make use of a wide range of techniques such as malicious software, logic bombs and networks of botnets that could result in fatal damage to an entire computer network of a state (Cornish, 2010, p.5). Consequently, IT networks have become an additional sphere of vulnerability where malicious state- and non-state actors are able to intrude and damage critical infrastructures. Hence, despite the opportunities that these networks of technology can provide, it creates an infrastructure of severe vulnerabilities at the same time. It is important to note that cyber space is understood as a new, but not entirely separate component of warfare environment since actions in cyberspace are mostly in conjunction with other forms conflict in the traditional domains of warfare (Cornish et al., 2010, p.9).

These vulnerabilities came into light when the first major cyber attack aimed against a state occurred in 2007. On the 27th of April, the nation of Estonia suffered a widespread cyber attack that effectively crippled the nation's electronic infrastructure (Boylan, 2017, p.218). This

event illustrated the striking fact, that serious destruction and damage on a state's stability is possible nowadays "without an enemy force ever setting foot on a rival nation's soil" (Boylan, 2017, p.219). In a very short amount of time and controlled from a distance, Estonia's entire critical infrastructure of digital civilian and military systems was affected. Consequently, nearly every citizen of Estonia felt the impact and the population reacted with hostility through riots that resulted in more than a hundred injuries and one death (Boylan, 2017, p.219). The Estonian attack in 2017 made clear that cyber attacks should be considered as powerful tools that potentially could have a devastating effect on a state's stability and safety. When the critical technological infrastructure of a state is under attack, blocked or infiltrated, civilians are at risk to be deprived of essential basic needs such as medical care, clean water and electricity (Gisel & Rodenhäuser, 2019). Despite the fact that cyber attacks are merely directed at computers rather than at people, cyber operations could potentially cause severe humanitarian costs. Essential civilian infrastructure such as power grids, hospitals and nuclear plants may be targets for disruption through digital means which could affect the well-being and security of lives of numerous civilians (Gisel & Rodenhäuser, 2019).

Considering these potential risks to civilian security, it becomes clear that there is a humanitarian need for the law to regulate and limit the effects of cyber warfare. One of the fundamental legal principles established in IHL in order to pursue the underlying goal to protect civilians during wartime is the principle of proportionality. This principle governs "the degree and kind of force used to achieve a military objective by comparing the expected military advantage gained to the expected incidental damage caused to civilians and civilian objects" (Pascucci, 2017, p.201). Hence, the principle of proportionality requires belligerents to balance the expected harm to civilians or civilian objects against concrete military advantages of an attack (ICRC, 2018, p. 38). In that sense, the IHL recognizes possible damage to civilian objects and civilian casualties, required that these are not excessive to the military benefits of an attack or operation. Notably, the principle of proportionality is not designed to exclude the possibility of any civilian casualties or damage to civilian objects," but only that which was excessive" (Jensen, 2013, p.206). As military operations are increasingly taking place in densely populated areas, the importance of the principle of proportionality is assuming growing significance for the protection and the security of civilians situated in armed conflicts (Gillard, 2018, p.3).

Legal rules and principles, such as the principle of proportionality, are generally forward looking by nature and ought to be applied in diverse and yet unknown situations (Pascucci, 2017). Nevertheless, the development of cyberspace as a new type of battlefield raises unique

issues in the application of international humanitarian law. The applying laws of IHL, which has its roots in the Hague Conventions of 1899 and 1907 and the Geneva conventions, were written decennia before the concept of cyber existed and numerous questions remain open about how existing legal frameworks can be applied to the currently developing phenomenon of cyberspace (Diamond, 2014). The norms and rules designed in this legal framework were built in a period when warfare was defined by the use of kinetic force in a physical world. However, cyber attacks are not likely to cause physical damage and rather generate disruptions in cyberspace, such as temporary inability to access systems or manipulation and loss of data. Subsequently, as the traditional application of the IHL rules and principles are based on kinetic effects such as death, physical damage and injury to civilians, some of the basic assumptions and fundamental principles underlying the IHL framework are likely to come into question when applicated on cyber warfare (Diamond, 2014) (Pascucci, 2017).

The framework of IHL will only apply to those cyber operations that exceed the legal threshold of an "attack" in "armed conflict" and will not be applicable to the ones that fall outside the status of an armed conflict (Schmitt, 2012, p.287). However, because of specific technological characteristics of cyber activities and the situation wherein they are launched, cyber attacks are often considered to fall outside the threshold of armed attack or armed conflict (Waxman, 2011, p.421). In that sense, cyber attacks are governed under IHL, only if the attacks reach the threshold of an armed attack in armed conflict. Nevertheless, the rapid technological changes to military weaponry is likely to increasingly effect military affairs and to make substantial impacts on the prosecution of war (Liles et al., 2012, p.169). As stated by Forge (2012), the provision of new weapons requires continuing justification as weapons are the means to harm (p.9). From a security perspective, the principle of proportionality established in IHL plays a fundamental role in the protection of human rights and security due to its role in balancing the costs of civilian losses and the needs of a military operation.

Therefore, this thesis will analyze the challenges posed by new methods used in cyberspace on the principle of proportionality from an international humanitarian law perspective, in order to build further on a broader understanding of the principle of proportionality in military operations using new means and methods of warfare. By providing research on the principle of proportionality, this thesis will contribute to academic literature with a comprehensive understanding of the principle of proportionality in the age of cyber that aims to support the existing knowledge on international security- and legal perspectives. The research question that derives from this is:

"How can the principle of proportionality protect civilians from the effects of military cyber operations?"

In order to answer this question properly, four sub questions will be answered in the first part of this thesis regarding the role of the principle of proportionality in protecting civilians during war:

- How is the principle of proportionality traditionally established in the international legal framework?
- How can cyber attacks reach the threshold of the *jus ad bellum* 'armed attack' and the *jus in bello* 'armed conflict'?
- How is the principle of proportionality established in military security perspectives?
- How can cyber operations cause physical harm to civilians and civilian objects?

Academic Relevance

The field of cyber security is rooted in traditional computer science. However, as a consequence of rapidly evolving computer technology and the increasing dependence on the internet in a digitalized society, the field of cyber security requires a cross-disciplinary research approach. Therefore, this thesis will contribute to the academic literature on cyberwarfare and the applications of traditional rules and norms by providing a multidisciplinary research through legal- and military security perspectives on the principle of proportionality in cyber operations. Today, broad consensus is reached among scholars that IHL applies to cyber operations during armed conflict (Schmitt, 2019, p.2). With the United Nations Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of International security (UN GGE), a number of countries expressly acknowledged the applicability of IHL to cyber operations which marked an important step in the effort to clarify how such operations can be constrained by international law (Schmitt, 2019). The UN GGE characterized the principles of "humanity, necessity, distinction and proportionality" as "established international law principles" that "govern the conduct of cyber hostilities during armed conflicts" (Schmitt, 2019, p.4). In this respect, it is not any longer a question of 'whether' IHL is applicable to cyberspace but merely a question of 'how' existing IHL rules can be applied adequately to the realm of cyber warfare.

As stated by Pascucci (2017), "the existing principles that govern the law of war should not be abandoned in the era of modern warfare, the traditional rules must rather be applied in novel ways and be rethought" (p.201). Therefore, this thesis will further build on the existing

literature, case law and the extensive ongoing debates in academic writings on the rule of proportionality in order to provide further clearance on the application of the principle to military cyber operations. In the article of Gillard (2018), the author extended the academic literature on this topic, with an extensive research on the principle of proportionality in the conduct of hostilities. Gillard (2018) notes that the research does not address the questions raised by the principle of proportionality in the realm of cyberattacks because this is beyond the scope of the article and stressed the need for further research elsewhere. It is valuable to develop a common interpretation of proportionality in cyberspace under international law, as it is likely that this principle will be tested by the characteristics of new weaponry used in military operations. Therefore, the aim of this thesis is to build further on this notion and support the existing academic literature by providing a comprehensive analysis of the application of the principle of proportionality in military cyber operations.

Societal Relevance

Weapon innovation generates new ways of causing harm to civilians and civilian objects, by new methods of killing people and destructing property (Eichensehr, 2015). Because of rapidly developing technological developments in military weaponry, the principle of proportionality is likely to obtain greater relevance to the conduct of armed conflicts due to its balancing character among humanitarian- and military interests in the novel cyber domain of warfare (Pascucci, 2017). As noted by Roscini (2010), computer networks have become the 'nerve system' of civilian and military infrastructures, "incapacitating them means paralyzing the country" (p.87). This can be illustrated by the impact of the Internet of things (IoT), which is fast developing as a distributed system for creating value out of data, that enables heterogeneous physical objects to share information and coordinate decisions (Lamas et al., 2016, p.16). In this respect, the IoT is redefining interactions between people and machines and optimize the development and distribution of certain products and services (Lamas et al., 2016, p.16). The IoT is increasingly influencing both civilian and military applications. In the military environment, the IoT can be applied to various military equipment such as vehicles, supplies and even to weapon systems to improve the efficiency and effectiveness of logistic operations (Wrona, 2015, p.1). However, "many such network-enabled objects have already been demonstrated to have significant security flaws and vulnerabilities" and in this regard, IoT devices present a new attack surface in military IT systems (Wrona, 2015, p.1).

By this, IoT weapons would be attractive targets for hostile actor's malware as a hacker could potentially take over control of a certain military IT system and let it operate up to its

own desires (Scharre, 2018). This development could potentially have striking effects on civil society in armed conflict since hacked autonomous weapons can cause severe unforeseen harm to civilians. In this respect, the interpretation of the principle of proportionality as civilian protecting principle, comes into question since fully autonomous weapons are not able to make decisions on ethical and legal considerations as reasonable military commanders do in assessing the principle of proportionality before launching a particular attack (Kosmyna, 2018). Besides, as stated by Gillard (2018), "as military operations are taking place with increasing frequency in densely populated areas, the rule of proportionality has assumed ever greater significance for the protection of civilians" (2018, p.3). Hence, in order to protect the civilians in armed conflict, it is crucial that armed forces comply with the principle of proportionality which assess the balance between military necessity and humanitarian security. Therefore, it can be considered valuable to examine the principle of proportionality as fundamental part of the IHL framework that protects civilian society in armed conflicts.

Research guideline

This thesis is structured in the following manner to answer the research question properly. At first, the theoretical framework chapter provides a brief overview of the theory of Just War as this theory has played a critical role in evaluating the moral and ethical use of new weaponry throughout the history of modern warfare. The fundaments of the Just War condition of the principle of proportionality will be illustrated in the *jus ad bellum* and *jus in bello* approaches. In the Research Design section, the methodology, data collection, case studies and limitations of the research will be explained and justified. In the third chapter, the principle of proportionality will be examined first from a legal- and military perspective, with emphasis on the application to the cyber domain of warfare. In order to examine the actual potential harm on civilians caused by cyber attacks, the literature review will provide a section dedicated to how cyber attacks can cause physical harm to civilians or civilian objects. Thereafter, an empirical analysis will be made of the application of the principle of proportionality in military cyber operations through two selected case studies in order to examine the empirical difficulties and opportunities of the principle of proportionality in cyber warfare. In the concluding section of this research, the main research question and its sub questions will be answered, aiming to incite further research on the application of traditional war regulation to the military use of cyber means and measures.

1. Theoretical Framework

1.1The Just War Theory

Without legal and ethical constraints on the decision to wage war and its conduct, war is nothing more than the application of brute force that is "logically indistinguishable from mass murder" (Bellamy, 2006, p.1). The Just War theory presupposes that war can potentially cause immense human suffering, however sometimes unavoidable due to the human psychology (Schulzke, 2017, p.1). Therefore, Just War theorist have sought to create conditions that are aimed to minimizing the human suffering during the conduct of war (Schulzke, 2017, p.1). In other words, the theory provides a justificatory framework that shapes one's judgements about war consisting of a meaningful language that soldiers and politicians should use to legitimize their actions in times of war (Bellamy, 2006, p.2). Besides providing a framework of legitimizing war, the Just War theory constrains and enables certain types of activity in war. To illustrate, Bellamy refers to Waltzer (1997) who stated that "professional soldiers remain sensitive to those limits and restraints that distinguish their life's work from mere butchery" (Waltzer, 1977, p.45 & Bellamy, 2006, p.2). The Just War theory deals with the question of how and why wars are fought and how they can be morally justified.

To determine whether a war is morally justified or not, the Just War theory lays down a series of conditions and if the war violates any of these conditions, it can be considered as an unjustifiable war (Hurka, 2005, p.35). These conditions can be distinguished into two major bodies of the Just War theory, the *jus ad bellum* and the *jus in bello*. The conditions laid down in the former concerns the resort to war and are directed to political leaders deciding "whether initiate war or whether to respond to another state's doing so with military force of their own" (Hurka, 2005, p.35). The conditions established in the latter, *jus ad bellum*, concerns the means used to fight war (Hurka, 2005, p.35). These conditions are directed at political leaders as well, who should make solely tactical decisions that are morally allowed according to the *jus in bello* parameters on ethically conducting war and using force (Hurka, 2005, p.35).

The application of the Just War theory on the new weaponry of cyber warfare has been discussed in academic literature. For instance, Randall Dipert (2010), questions whether the Just War theory is straightforwardly applicable to the conduct of cyber warfare (p.395). The author implies that traditional discussions on the morality of war has been understandably motivated by the lethal character and massive destructiveness of war. In cyberwarfare, Dipert argues that consequences of cyber attacks could be lethal and physical destructive, but it will

often not be like that (p.386). Dipert refers to the United Nations (UN) Charter, where an 'armed attack' is only considered justified when a state defend itself before the Security Council takes action (UN Charter, 1945: Ch.7, Article 51). Hence, Dipert states that this article can be understood, "to designate soldiers using 'arms' as artifacts for inflicting injury, death, or physical destruction of objects" and therefore, considering cyberwarfare as an 'armed attack' is an overstretch of the term since cyber attacks rather may involve aspects of damage or harm the functioning of information systems and not harm physical objects of persons. (Dipert, 2010, p.395). Dipert concludes with the notion that relevant entities in cyberwarfare such as software systems and information entities, are very unusual in comparison with the ordinary objects of daily life, and for that reason not complying with the traditional emphasis on damage to human lives and civilian objects as described in Just War theory (Dipert, 2010, p.406).

Another article that questions the application of the Just War theory on cyberwarfare is written by Lin, Allhoff and Rowe (2002). These authors argue that the Just War theory cannot be adequately applied to the characteristics of cyberwarfare for the similar reason as posed by Dipert on the historically posed characteristics of the 'just cause' for war, a defense to aggression (2010). Lin, Allhoff and Rowe (2002) imply that aggression should be understood as an action whereby human lives are directly in jeopardy, which becomes difficult to justify in a military response to a cyber attack that does not cause kinetic or physical harm as in the 'Clausewitzian sense' (p.1). In fact, the authors question the seriousness of cyber attacks in comparison with conventional kinetic attacks, since cyber attacks do not directly target lives (Lin, Allhoff & Rowe, 2002, p.1). According to the authors, aggression in cyberspace is not tied to actual physical harm or threat to lives, and rather cause the disruption of a computer system or infrastructure that directly kills no one, therefore it is unclear how to understand cyber attacks in traditional military ethics according to the authors (Lin, Allhoff & Rowe, 2002, p.2).

However, despite there is no evidence of deadly victims directly caused by cyber weapons to date, this does not mean that these sorts of weapons are incapable of doing so. On the contrary, due to rapidly technological developments of military weaponry, the potential physical effects of cyber attacks could make them just as lethal as conventional kinetic attacks (Dayem, 2018, p.5). According to Dayem (2018), cyber attacks can be considered as acts of war because of the analogy to the consequences caused by conventional kinetic attacks (p.5). This view is supported by Taddeo (2012), who notes that despite the conditions of the Just War theory are not as easily straightforward applicable to cyberwarfare as traditional warfare, "It would be misleading to disregard the Just War theory when analyzing cyberwarfare. The ideal

of just warfare provided by the just warfare theory and its principles remain valid even when considering this new kind of warfare" (p.214). When the Just War theory is applied to cyber warfare, a human being, who suffers harm caused by a cyber attack and an informational infrastructure that is disrupted by a cyber attack, "are both to be considered as the receiver of the moral action" (Taddeo, 2012, p.215). This view is supported by Davis (2001), who states that the Just War theory may offer conceptual guidance concerning the legal and ethical use of cyber attacks. The author notes that despite some difficulties in applying the Just War theory on cyberwarfare, the Just War theory provides a framework for moral consideration in modern warfare and a systematic approach through a common language in order to analyze the ethical dilemmas that are posed by new means and methods of warfare (Davis, 2001). Yates (2013) concludes that new technologies have changed the character of war throughout history, and it is undeniable that cyber weaponry has and will continue to do so as well. Therefore, it can be argued that the Just War theory remains applicable in order to determine whether a resort to war or the conduct of war by the use of new technologies is justifiable. This research will be built further on this argument in order to examine the Just War requirement of proportionality in the context of military cyber operations.

1.2 The principle of proportionality established in the jus ad bellum and the jus in bello

1.2.1 Jus ad Bellum

A just war is supposed to be proportional in responses to aggression (Forge, 2009). In this sense, the costs of war must never greatly exceed the anticipated military benefits. The principle of proportionality is established in both *jus ad bellum* and *jus in bello* to impose moral and legal constraints on the use of force by parties to an armed conflict. In *jus ad bellum*, proportionality has a dual role: it provides to identify situations in which unilateral force is permissible and it serves to determine the magnitude and intensity of military action (Cannizzaro, 2006, p.781). The principle of proportionality is part of the *jus ad bellum* as one of the six preconditions for the morally justified resort to war by an armed group or state against another. The six preconditions to undertake a morally justified war are "(1) by a legitimate political authority, (2) to achieve a just cause (3) as a last resort (4) with the right intention (5) with a reasonable chance of success (6) the harms caused by war are not disproportionate to the relevant military benefits that the war will produce" (Haque, 2012, p.2). Illustrated in the article of Haque (2012) on proportionality in war, the 'relevant harms of war' include loss of life and injury of civilians, destruction of civilian property, damage to the natural environment and infringements of the territorial integrity or political independence of other states. Additionally,

the resort to armed force will be considered disproportionate if it results in widespread malnutrition, poverty or disease among the civilian population, however less severe economic harms might not affect proportionality. Hence, states can unilaterally resort to force in case of self-defense when the concerning state has been the victim of an armed attack. As stated by Cannizzaro (2006), this does not mean that the right of self-defense is an open-ended instrument, but only has the aim of "repelling armed attacks and provisionally guaranteeing the security of a state" (p. 782).

Nevertheless, defensive force can only be used by a state to counter armed attacks that requires a certain threshold of intensity. Below that threshold, minor types of force will fall short on the notion of "armed attack" and cannot be met with a forcible response of self-defense (Cannizzaro, 2006, p.782). In this view, the right of self-defense does not protect individual states to any offensive use of force, and rather considers the use of force as appropriate solely in response to acts of aggression which objectively endangers its security to the extent that it is necessary to repel them in order to protect its national security (Cannizzaro, 2006, p.782). Once an armed response in self-defense occurred, it must be questioned whether the type and scale of the armed response, can be considered as appropriate in the response. Proportionality in this view can be measured by a quantitative and a qualitative test. The former requires the conformation to quantitative features of the attack, such as the type of weaponry, the scale of action and the magnitude of damage (Cannizzaro, 2006, p.784). The latter test ought to seek whether the means employed are appropriate in relation to the aim sought by the response, in other words, whether the response is necessary and appropriate to repel the attack, and which entails acceptable side-effects (Cannizzaro, 2006, p.784).

1.2.2 Jus in Bello

The principle of proportionality is one of the three *jus in bello* conditions, complementary to the discrimination- and the necessity condition. Proportionality in *jus in bello* refers to the condition that collateral killing of civilians is prohibited if the resulting civilian deaths are disproportionate to the relevant military advantages that will be gained by the attack (Hurka, 2005, p.36). Thereby, the proportionality condition under the *jus in bello* allows for instance the bombing of a vital munitions factory that will unavoidably kill civilians but forbids killing thousands of civilians as a side effect of achieving a military goal (Hurka, 2005, p.37). According to Haque (2013), proportionality in military operations must be determined by "comparing the military advantage a combatant intends to achieve to the loss of life or injury to civilians, damage to civilian property and damage to the natural environment that the

combatant foresees but does not intend either as a means or as an end" (p.3). Hence, the primary concern of the principle in the *jus in bello* is not merely the preservation of international peace and security but rather the protection of humanitarian values, in particular the limitation of the suffering of non-combatants in situations of armed conflict (Steenberghe, 2010, p.119).

In this respect, the logic behind the proportionality under *jus in bello* is inspired by a different logic than under the *jus ad bellum*, as described in the previous section. As noted by Cannizzaro (2006), the legal regulation of the *jus ad bellum* use of force is based on "a superior right of the attacked state in regard to the attacker", whereas the legal regulation of the *jus in bello* means and methods of warfare is dominated by the "parity of the belligerents and by the concomitant principle of the respect owed by each of them to interests and values of a humanitarian nature" (p.785). Another difference between the principle proportionality in *jus ad bellum* and *jus in bello* is that proportionality in *jus in bello* cannot "logically be measured by reference to the ultimate goals of a military mission, but rather to the immediate aims of each single military action" (Canizzaro, 2006, p.786). Furthermore, the scope of damage, a condition for assessing proportionality under the *jus ad bellum* as well, is viewed from a different perspective under *jus in bello.* In the latter, the emphasis is on damage caused to individuals and individual objects as such, rather than damage caused to a particular state as unit of analysis (Steenberghe, 2010, p.119).

2. Research Design

2.1 Choice of methodology

The aim of this research is to provide a broad understanding and clarify the definition of the principle of proportionality, examine the history of the current principle, assess the status quo in the age of cyberwarfare and eventually illustrate the potential future of the principle. In order to answer the research question that derived from this purpose properly, this thesis will follow a qualitative research methodology based on a literature review of legal and non-legal documents, combined with a case study design in order to explore the role of the principle of proportionality in the empirical world. The methodology of literature review allows this thesis to explore the universe of publications and case law on the application of the IHL principles, the principle of proportionality in particular, in military cyber operations. By integrating perspectives from various empirical findings and publications, the literature review section of this research provides an interdisciplinary understanding on the principle of proportionality in military cyber operations. As stated by Snyder (2019), "literature reviews are useful when the

aim is to provide an overview of a certain issue or research problem" and "is conducted to evaluate the state of knowledge on a particular topic" (p.334). In addition, Snyder (2019) argues that a literature review methodology is valuable to map the development of a specific research field over time. In this regard, conducting a literature review based on legal and non-legal documentation allows this research to develop an interdisciplinary understanding on the knowledge of the principle of proportionality and its application in military cyber operations.

Furthermore, this thesis will examine the principle of proportionality in empirical context by two case studies. The key characteristic of a case study is to provide an in-depth examination of a current complex phenomenon. The conditions for a case study method have been explained by Yin (2014) as: " doing a case study would be the preferred method, compared to the others, in situations when (1) the main research questions are "how" or "why" questions; (2) a researcher has little or no control over behavioral events; and (3) the focus of study is a contemporary (as opposed to entirely historical) phenomenon." (p.16). In this regard, a case study method fits the purpose of this thesis to explore the understanding and application of the principle of proportionality in military cyber operations as this research provides an exploring 'how' question, no control is possible over behavioral events and the focus of the research is the contemporary application of the principle of proportionality. Hence, a case study design will provide the opportunity to gain an in-depth understanding of certain phenomena within an empirical context and explore complex social issues from a legal and security perspective (Langebroek et al.,2017). According to Langebroek et al. (2017), "the application of a case study method in empirical legal research could provide analysis concerning how legislation is 'understood', 'applied', or 'misapplied'" in the empirical world (p.101). In this respect, a case study methodology enables this research to explore the principle of proportionality and illustrate how this legal principle can be applied in the empirical realm of cyber.

A cross-case analysis methodology enables this research to compare the commonalities and the differences in the two case studies with the application of the principle of proportionality as unit of analysis (Yin, 1981, p.108). By examining case knowledge across two separate events in the realm of cyberwarfare, this research aims to provide an in depth understanding of accumulated knowledge from comparing the application of the principle of proportionality in multiple settings. Since the development of cyber measures in military operations is a relatively novel phenomenon, there are just a few precedents where cyber measures affected the physical world. The selected cases are both cyber-warfare incidents that included the involvement of states and caused physical damage via cyber means rather than

solely disrupted the digital realm. The two cases will be compared in a most different case design where the two cases differ as much as possible, as the selected cases are very different units in many aspects (Langebroek et al., 2017). The selected cases do not share a common geographical area, cultural tradition or historical and economic development. More importantly, the Stuxnet case occurred in peacetime and the IDF-Hamas case occurred during wartime. The shared variable is the presence of a cyber attack which affected the physical realm which questions the principle of proportionality. By exploring the application of the principle in these two most different cases, a broader understanding of the application of traditional legal rules in the novel domain of cyberwarfare can be provided.

Regarding the ability to generalize the outcomes of this research, legal rules and principles, such as the principle of proportionality, are generally forward looking by nature and ought to be applied in diverse and yet unknown situations (Pascucci, 2017). The application of the principle of proportionality is very much case specific, however, it will be valuable to create a broader understanding of the principle in order to create generalized understanding of the principle of proportionality in the novel realm of military cyber operations. As military operations will increasingly use cyber measures to gain military advantages, it is essential to explore the application of traditional norms and rules in the rapidly evolving cyber space. Hence, the aim of this research is to contribute to a general understanding of the application of the principle of proportionality in military cyber operations by looking at the patterns, challenges and opportunities in both cases.

2.2 Data collection

The data used in this research will be selected through triangulation of various relevant open sources in order to answer the research question properly. The convergence of information collected from different type of sources, enables this research to gain a multidisciplinary perspective on the principle of proportionality. The selected data will merely exist of academic papers on the principle of proportionality from legal and military perspectives, official reports released by the ICRC on the application of IHL on cyberwarfare, case law from the International court of justice and the International Criminal court. In addition, newspaper articles and blog posts written by professionals from various relevant academic fields will be used as additional sources to support the purpose of this research. In this respect, data triangulation enables this research to provide a clear and comprehensive understanding of the principle of proportionality applied in military cyber operations.

2.3 Case selection

2.3.1 Stuxnet

The Stuxnet attack is known as the "most complex malware ever written" and has intrude Iranian computers in order to infect the country's uranium enrichment program in June 2009 (Sussman, 2017, p.494). Stuxnet is a particularly interesting case since it is "one of the first known weapons, and the most impactful one to date, to jump the gap from wreaking mere cyber-havoc to wreaking physical destruction" (Jenkins, 2013, p.69). Stuxnet is a highly sophisticated computer worm that behaves differently from the usual malicious malware, instead of stealing information or hijacking the targeted computers, the Stuxnet worm escaped the digital realm to force physical destruction on the equipment the computers controlled (Dunn Cavelty, 2010, p.111) (Zetter, 2014). The Stuxnet worm was "hunting for something in particular", it did not steal information infect computers to launch further attacks, rather it particularly looked for a very specific target: the Siemens' *Supervisory Control and Data Acquisition* (SCADA) systems that are used to control and monitor industrial processes (Dunn Cavelty, 2010, p.11). In this regard, Stuxnet stood out as a new kind of weaponry as it was designed to cause physical damage, *via* cyber means to the Iranian power plants (Singer, 2015, p.84).

2.3.2 IDF-Hamas

In May 2019, the principle of proportionality additionally came into question when an unprecedented event happened in the Israel – Hamas violence. The Israeli Defense Force (IDF) claimed that it bombed and partially destroyed a building in Gaza that was allegedly the base of an active Hamas hacking group or even the headquarters of the Hamas cyber forces. This assault is the first true example of a kinetic attack that was launched in direct response to a cyber attack. The commander of the IDF Cyber Division stated that the cyber attack posed by Hamas on Israel "was aimed at harming the quality of life of Israeli citizens" (Doffman, 2019, par.1). In response, the IDF bombed Hamas' cyber headquarters that resulted massively destruction of the targeted building in the Gaza strip. In this respect, the attack raises serious questions about the proportionality of the IDF response as the physical response to a cyber attack is an unprecedented event to date. By analyzing this case study, this thesis aims to examine the challenges and opportunities of the principle of proportionality in a case as such.

2.4 Operationalization

In this research, the term 'cyber-warfare' is used to refer to "means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL" as used in the ICRC report of 2013 on the application of IHL to cyber-warfare (p.1). Despite the fact that there is no international consensus on the definitions for 'cyber attack', 'cyber-operation' and 'cyber weapon', there is some form of agreement that these terms refer to "the execution of malware with the objective of denying, disrupting, degrading, destroying or manipulating information systems or the information resident on them" (Iasiello, 2015, p. 24). In this research, the definitions illustrated by Iasiello (2015) in the Military and Strategic Affairs journal will be adopted to define 'cyber attacks' and 'cyber weapons'. Cyber attacks are considered as "actions taken through computer networks designed to deny, degrade, disrupt, or destroy an information system, an information network, or the information resident on them." (Iasiello, 2015, p.24). Besides, a cyber weapon will be considered as "a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings." (Iasiello, 2015, p.24). The term 'cyber operation' will be used as described by Romanosky & Goldman (2016) stating that "cyber operations include the use of cyber capabilities such as computers, software tools, or networks: and have primary purpose of achieving objectives or effects in or through cyberspace" (p.11).

2.5 Limitations

It is important to note that research on the principle of proportionality specifically, should be considered in a framework of numerous ongoing debates on the application of traditional rules and principles to the domain of cyberspace rather than in isolation. A critical debate in the field of cyber security that relates to the principle of proportionality is on the legal condition of 'attribution'. Identifying the responsible actor of a cyber attack is essential for determining political or legal action in response to the attack. Attributing a cyber attack is likely to be highly complicated because of the complex technical nature of cyberspace (Tsagourias, 2012). Besides severe technical difficulties such as anonymity and traceability, there is no clearance yet on the desired level of evidence to attribute a cyber attack to a certain actor. However, knowledge and evidence on the actor behind a cyber attack and its intentions is crucial to determine the political or legal action that must be taken. According to Petkins (2016), attribution of cyber attacks is extremely difficult, however, necessary for purposes of proportionality. Particularly, in the *jus ad bellum* condition of proportionality in self-defense,

since any "action taken against a state that did not actually perpetrate a cyber-aggression is disproportionate *per se*" (Petkins, 2016, p.1456). In this respect, knowledge on the perpetrator is crucial in order to avoid the violation of the right of self-defense.

Furthermore, Kremer's article (2014) on militarizing cyber security, the author argues that cyberwar can be approached from two different legal perspectives: in a narrow and an expanded way (p.230). This research will solely focus on the narrow legal perspective on cyberwar. A narrow approach follows the logic of the 1949 Geneva conventions and the legal body of IHL, distinguishing between justifiable and unjustifiable military- and civilian targets in a situation of armed conflict (Kremer, 2014, p.230). In this sense, the narrow approach understands military cyber operations in view of the *jus in bello* and the *jus ad bellum*, emphasizing the conduct- and the mechanism of justifications to engage in warfare. In this respect, this research will not elaborate on the expanded legal perspective on cyberwar. The broad definition given by Kremer (2014) comprise "any kind of cyberattack against a nation's civil and military infrastructure from not only any kind of actor, but also acts of industrial espionage, hacking, net-activism etc." (p.230). Despite of the importance of the discussion of attribution in cyberspace and the various ways of conducting cyber attacks from broad legal perspective, this research will not further elaborate on these topics due to the scope and timeframe of this research. Hence, although the principle of proportionality is part of a broader legal framework and cannot operate isolated from a broader network of rules and principles, it is valuable to provide an in-depth understanding of the principle of proportionality in a narrow legal perspective in order to contribute to the academic literature about the application of the IHL principles in context of cyber warfare.

3. Protection by the Principle of Proportionality in War

3.1 The principle of proportionality from a legal perspective

3.1.1 History of the principle of proportionality in international law

The proportionality condition established in the Just War theory is a concept found in various areas of public international law, including the areas of trade law, international human rights law, rules that govern states' resort to the use of force as well as the IHL framework (Gillard, 2018, p.6). Before the establishment of the principle of proportionality in IHL is illustrated in the next section, this section provides a brief history of the principle of proportionality in the legal realm. The practical legal implementation of the principle of

proportionality, represents a key aspect of contemporary legal thought and has been developed throughout early history (Engle, 2012, p.2). The earliest source of the principle of proportionality in law appears in Aristotle's fifth book, where the author proportionately measures distributive justice in the right relationship between the state and citizens (Engle, 2012, p.4). The general and vague thoughts of Aristotle on proportionality has been increasingly made concrete by Marcus Cicero and Thomas Aquinas in the law of self-defense. Aquinas argued that there are certain conditions to the just use of force in self-defense, the use of force must be just; necessary; not be excessive and the be exercised in respect to the rules of sovereignty (Engle, 2012, p.2). The theory of Aquinas on self-defense, became one of the fundamental principles of the international law made by Grotius (Engle, 2012, p.4).

Grotius has translated the concept of proportionality into modernity and "links the idea of justice as proportion to the idea of interests, balancing as a method for dispute resolution" (Engle, 2012, p.5). As stated by Engle (2012), Grotius unified the ancient concept of proportionality by Aristotle, the medieval concept of proportional self-defense by Cicero and Aquinas, and the modern concept of balancing interests (p.5). In that sense, the principle of proportionality emerged as a universal principle for resolving conflicting fundamental norms (Engle, 2012, p.2). As stated by Nolte (2010), proportionality is an argument for the claim that there is a common language between different legal systems, even a substantive commonality, but at the same time it leaves room for specificities in legal systems. In fact, the principle can be understood as a principle, respectively as a rule, depending on the context and case in which it is applied (p.247). As the principle of proportionality is continuously balancing possibilities and is seeking for the 'right' proportion, it provides a more rational perspective on restricting rules. On the one hand the principle of proportionality invites an 'objective' and 'neutral' promise of the law, and on the other hand the process of applying the principle of proportionality is a 'value based' consideration (Nolte, 2010, p.247).

The early development of the principle of proportionality in international law practices is illustrated by the *Naulilaa* arbitration. During this case of interstate arbitration, Portugal established a special arbitral tribunal to hold Germany responsible for the attacks on the Portuguese post of Naulilaa in Angola which a substantial number of people were killed and caused severe property damage (Quillin, 1926) (Nolte, 2010, p.249). These attacks, which took place in October 1914, were conducted by Germany, in response to the killing of three members of a German delegation by Portuguese troops. The arbitral tribunal decided that the attacks conducted by Germany were being considered as excessive and illegal and that there was an

obvious disproportion between the incident at Naulilaa and the reprisals which followed performed by Germany (Nolte, 2010, p.249). The arbitrators decided that an armed reprisal is only justifiable under international law when it meets the requirement of proportionality in respect to the unlawful act which provoked the reprisal (Kretzmer, 2013, p.253). Nowadays, this decision is considered to be a landmark case in public international law and strongly connected with the requirements of a justifiable forceful reprisal, with the principle of proportionality as of one of the most important requirements (Zollmann, 2016).

3.1.2 Proportionality in International Humanitarian Law

This sub section will focus on the establishment of the principle of proportionality in IHL. In order to answer the research question adequately, it is crucial to analyze the principle of proportionality in this legal framework since the IHL legal framework aims to protect people who take no part in hostilities from suffering and to pose restrictions on the means and methods of warfare in order to limit humanitarian issues arising from an armed conflict. Established in the framework of IHL, the principle of proportionality prohibits attacks against military objectives which are expected to cause excessive damage to civilian objects or injury to civilians, or a combination thereof, in relation to the concrete military advantages anticipated. In that regard, the proportionality principle seeks to limit excessive damage caused by military operations, by the requirement that the effects of the means and methods of warfare used shall not be disproportionate to the military advantage that is sought by the attack. The principle of proportionality in attack is codified in Article 51(5)(b) of the Additional Protocol to the Geneva conventions of 12 August 1949 which relates to the Protection of Victims of International Armed Conflicts and repeated in Article 57 of the same Additional Protocol. In Article 51, the principle of proportionality is described in the context of indiscriminate attacks and the prohibition of these form of attacks.

In Art. 51(5)(b) is stated that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (ICRC, 1977). In this sense, attacks that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof" would be considered as unjust due to its excessive character in relation to the "concrete and direct military advantage anticipated". After, in Article 57(2)(a)(iii) and Article 57(2)(b), the principle of proportionality is framed in the context of precautionary measures that must be taken to be considered as a justified act within the context of IHL. Art. 57(2) (a) states that those who decide upon an attack,

shall refrain from launching any attack that is expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated (ICRC, 1977). In addition, in Art. 57(2)(b) it is laid down that an attack "shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (ICRC, 1977).

'Precautions in attack' refers to those who plan or decide upon an attack, are required to "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection" (Schmitt, 2011, p.92). In this respect, the ones who plan or decide upon an attack, must take reasonable choices in the means and methods used in an attack in order to minimize civilian harm weighed to the anticipated military advantage of the attack. Hence, as stated by Barnidge (2011, p.278), Art. 57(2)(a) provides a context for the principle of proportionality at the authorization stage while Art. 57(2)(b) upholds the principle at a stage where an attack was already determined as proportionate, yet considered as disproportional when it becomes apparent that the expected damage to civilians and civilian objects will be excessive to the anticipated military advantage. As noted by Gillard (2018), the articles of AP I do not provide guidance on how to understand the foreseeability or causation for the proportionality determination. The former considers the question whether the harm by the attack could be *expected*, the latter considers the question whether the expected harm is directly *caused* from the attack (Gillard, 2018). Interpretations of other areas of public international help might give some assistance, however in other areas of law causation and foreseeability are merely considered after the event, "at the stage of determining the existence of a wrongful act and awarding reparations" (p.14). In contrast, in the proportionality assessment, the questions of foreseeability and causation must be considered beforehand of the event, in the earlier stage of "identifying the expected incidental harm to be balanced against the anticipated military advantage" (Gillard, 2018, p.14).

Considering these regulations, which actors should comply with the principle of proportionality in armed conflicts? The restriction given in Article 51 AP I on attacks that violate the rule of proportionality is binding on every party to an armed conflict (Gillard, 2018, p.43). As stated by Gillard (2018), "the parties must take all necessary measures to ensure compliance with the rule by members of their forces at all levels" (p.43). The measures that

must be taken are (1) include an assessment of attacks when the rule have may been violated, (2) making legal advisers available to advise military commanders, (3) incorporating the rule of proportionality into military manuals, doctrines and rules of engagement, (4) establishing systems to gather and analyze relevant information on the context of the attack and ensure that this information is taken into account in the targeting cycle, (5) institutionalizing procedures to ensure proportionality considerations are taken into account throughout the targeting cycle, (6) conducting 'lessons learned' after attacks to inform future attacks, (7) addressing the rule of proportionality in training materials and scenario-based exercises (Gillard, 2018, p.44). In addition, Article 57 of AP I is specifically addressing an obligation to "those who plan and decide an attack" to comply with the principle of proportionality, which is an unusual approach according to Gillard (2018). The one's that plan or decide an attack are obliged to do everything feasible to verify that an attack against a military objective is not prohibited under the rule of proportionality.

The principle of proportionality is closely related to the other principles of IHL, in particular to the principle of military necessity and the principle of discrimination between combatants and non-combatants. In fact, the principles of distinction and proportionality complement each other in order to achieve a balance between military necessity and humanitarian concerns (Sari & Tinkler, 2019, p.4). Hence, in order to obtain an in-depth understanding of the principle of proportionality, it is essential to examine the principle of proportionality in relation to the principles of necessity and discrimination as well. By the principle of necessity, IHL recognizes that it is necessary for armed forces to use deadly force on their opponents in order to gain military advantages and overcome the enemy (Boogaard, 2019). This principle can be correlated the Just War *jus ad bellum* condition of 'last resort' (Haque, 2012, p.2). In this respect, it is legally permitted to use weapons and munitions against persons as much as it is necessary to win the war (Boogaard, 2019, p.21). In its strictest sense, the necessity principle in the law of force provides that states can only justifiably use military force in self-defense "when peaceful means have reasonable been exhausted, or when diplomatic enterprises would clearly be futile" (Haque, 2016, p.3).

The principle of discrimination is reflecting in IHL rules that prohibits adverse distinction in treatment of persons based on criteria such as gender, nationality, religion or political affiliation. All persons that are protected under IHL, should be treated with the same consideration by parties participating in armed conflict. In other words, every person affected by armed conflict is entitled to its fundamental rights and guarantees, without discrimination

based on the above-mentioned criteria. The principle of distinction can be distinguished into three components which are (1) the obligation to determine who may and who may not be attacked; (2) the ban on the use of indiscriminate weapons and (3) the prohibition on the indiscriminative use of otherwise discriminate means of warfare, resulting in indiscriminate attacks (Boogaard, 2019, p.23). The principle is codified in article 48 of API, which states that "Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives." (ICRC, 1977). In this sense, the principle of distinction protects the peaceful civilian population against the effects of hostilities and only permits attacks against the armed forces of the parties participating in an armed conflict.

Inherent to the principle of distinction and the principle of proportionality is the duty of parties in armed conflict to avoid 'collateral damage'. The term collateral damage refers to "unintentional or incidental injury or damage to persons or objects that are not lawful military targets" (Cronin, 2013, p.1). In other words, despite the well-established rule that military operations may not intentionally target civilians or civilian objects, the fact that civilian assets may be incidentally harmed during a military attack does not automatically mean that the attack is considered illegal (Gillard, 2018). Incidental damage as such is thus commonly referred to as 'collateral damage' (Gillard, 2018, p.227). In this regard, an attack resulting in civilian casualties or the destruction of civilian property does not make an attack illegal by itself, *per se*, it merely invokes the rule of proportionality (Gillard, 2018, p.277). Notably, collateral damage includes solely the expected civilian deaths, injuries and damage to civilian objects and no abstract effects such as stress, irritation, inconvenience or fear (Reece & Henderson, 2018, p.838).

Since the use of cyber means and methods in the conduct of war developing rapidly in the last decade, various debates have taken place whether this body of law is relevant and applicable to acts of warfare conducted by cyber weapons (Gill, 2015, p.367). Diamond (2014) states that the legal framework evolves slowly while new means and methods of warfare develop continually, and the battlefield is rapidly changing (p.69). Consequently, the process of adapting the IHL traditional legal framework to new cyber technologies used in armed conflicts is challenging (Eichensehr, 2015). Merely, because the application of the IHL rules and norms were designed to be applied on means and methods of warfare involving the use of kinetic force in the physical world (Diamond, 2014, p.70). The challenges of the application of IHL to cyber-warfare are discussed by the article of Gill (2015) as well. According to Gill

(2015), the IHL framework only applies when the conditions relating to the threshold of the existence of an armed conflict have been reached (p.367). Standalone cyber attacks are not likely to reach the thresholds for the existence of an armed conflict.

Furthermore, Gill (2015) argues that it is not likely that States would use massive stand-alone cyber attacks as main method to conduct in the event of an armed conflict (p.370). According to the author, it seems illogical that large-scale armed offensives carried out by a state against another state, would be limited to cyber means of warfare, as stand-alone cyber attacks do not enable States to destruct or effectively eliminate a target permanently or for a long period of time (p.370). An example that is given by Gill (2015) is, once a state aims to destruct a particular military capability, platform or critical installation, it would be difficult to pose long-term damage on the object by cyber means alone. Therefore, a state would rather strengthen its cyber techniques of warfare by use them in conjunction with traditional kinetic weapons (Gill, 2015, p.370). It is the conjunction with kinetic force, described by Gill (2015), that raise the consequences of cyber attacks to the required threshold of an armed conflict governed by IHL. The most likely scenario to fit into the qualification and definition of an 'armed attack' is when cyber operations would be used as a means of attack in conjunction with traditional kinetic weapons (Gill, 2015, p.378). In this regard, cyber attacks conducted by parties in armed conflicts must be governed within the context of an international armed conflict of IHL. Therefore, cyber attacks that reach the threshold of IHL as illustrated, must be governed by the principle of proportionality and considered unjustifiable when excessive damage is posed on civilians or civilian objects.

In this respect, the ICRC noted "In the ICRC's view, there is no question that cyber operations during armed conflicts are regulated by international humanitarian law – IHL – just like any other weapon or means or methods of warfare used by a belligerent in a conflict, whether new or old" (ICRC, 2013). Therefore, as the use of cyber operations in armed conflict can potentially have devastating humanitarian consequences, the ICRC state that it is considered as crucial to identify ways of limiting the humanitarian costs of cyber operations, and particularly reaffirm the relevance of IHL to the use of new technologies in armed conflict (ICRC, 2013, p.1). Because of IHL anticipate on advances in weapon technology and the development of new means and methods of waging war, there is no doubt according to the ICRC that IHL covers cyberwarfare. As stated by the ICRC, the key challenge raised by cyberwarfare is to ensure that the attacks are directly target military objectives and there must be a constant care to spare the civilian population and the civilian infrastructure. Moreover, "the

expected incidental civilian losses and damage must not be excessive in relation to the concrete and direct military advantage anticipated by the cyber attack" (ICRC, 2013). Hence, the principle of proportionality applies in a similar way to cyber attacks in the context of armed conflict as to any other type of attack if it expects to cause excessive damage to the civilian population. If the proportionality conditions cannot be met, the attack is unjustifiable under the conditions of the proportionality principle and must not be launched.

As illustrated above, a key requirement of cyber attacks to fall under the governance of IHL is to have a disruptive effect in the physical world, similar to the effects of traditional kinetic means and methods of warfare. In this regard, the principle of proportionality regulated by the framework of IHL, becomes relevant when a cyber attack causes incidental physical harm to civilians or civilian objects. The following sections will elaborate further on the capability of cyber attacks to cause physical harm and the consequences thereof in the context of international war regulations.

3.2 Kinetic vs. Cyber means of conducting warfare: reaching the threshold of an 'armed attack' or an 'armed conflict'.

3.2.1 Cyber attacks in the jus ad bellum

The *jus ad bellum* regulates the use of force by states in their national relations. As weapons become more technologically complex, determining whether a cyber attack can be considered as a use of force, becomes equally complex. However, as seen in the previous section, this determination is of imminent importance in order to decide whether the rules and principles of the law of armed conflict *jus in bello* and/or the law governing the use of force *jus ad bellum* apply to the act. The key rules on the use of force are to be found in the United Nations Charter of Rights and Freedoms (UN Charter). The UN Charter contains a prohibition of the threat or use of force in Article 2 (4) and two circumstances in which the prohibition of the use of force does not apply. The first is authorization by the Security Council to the use of forcible measures, acting under Chapter VII of the Charter. The second is that force may be used in the exercise of the right of individual or collective self-defense (Wood, 2013, p.352). Nevertheless, the Charter does not specifically define what constitutes 'use of force' or an 'armed attack'. The Charter was drafted and adopted in an era where warring nations exposed physical damage on adversaries primarily through kinetic attack: "bombs and bullets delivered by artillery and rifles that are the mainstay of conventional military combat" (Nguyen, 2013, p.1081). As illustrated by Nguyen (2013), the International Court of Justice (ICJ) provided

some clarity with regard to the traditional methods of war as well, referring to "aerial bombardment, ground assault, missile strikes and other territorial incursions" (p.1081). Also noted by Schmitt (2011), the term 'use of force' contains resort to armed force by a state, force levied by the military in particular (p.73). Thus, noted by Schmitt (2011), "armed force includes kinetic force – dropping bombs, firing artillery, and so forth" (p.73). In this respect, the traditional 'use of force' is characterized with the use of lethal or potentially lethal force against the population of the adversary.

With respect to cyber attacks in the *jus ad bellum*, the definitional boundaries of an 'armed attack' remain blurred. As noted by Nguyen (2013), international law provides little direct guidance to determine whether a cyber attack rises to the level of force or armed attack (p.1080). To illustrate this, the author provides an example of the Chinese military program of cyber attacks. However, denied by the Chinese government, the US accuse Chinese hacker groups of the theft of hundreds of terabytes of data (Sanger, Barboza & Perlroth, 2013, par. 7). The White house stated "We have repeatedly raised our concerns at the highest levels about cyber theft with senior Chinese officials, including in the military, and we will continue to do so", and plans on a more aggressive defense against Chinese hacking groups (Sanger, Barboza & Perlroth, 2013, par. 7). Despite the serious accusation, as argued by Nguyen (2013), this type of cyber attack is unlikely to be seen as an act of ware and will rather be seen as espionage, which is neither regulated under the rules and principles of international law (p.1082). In this respect, cyber attacks that cause harm in the virtual realm alone rather than physical harm, are not likely to be considered as an act of war governed under the *jus ad bellum.* However, cyber attacks can potentially generate consequences analogous to effects caused by kinetic force in the physical realm. Therefore, it is important to question how international law should treat cyber attacks that directly result in physical harm to individuals under the *jus ad bellum*.

According to Schmitt (2011), it would be "no less absurd" to suggest that cyber attacks that generate effects similar to those caused by kinetic force, lie beyond the reach of prohibition under international law. Therefore, cyber operations that equates to armed force in the sense that the attacks directly cause physical harm to individuals or objects, should therefore be considered as a use of force (p.573). It is important to note that cyber operations that involves economic or political pressure is not considered to be a prohibited use of force. This is determined in the proceedings leading to the UN general assembly's declaration on Friendly Relations where the question was raised whether 'force' included 'all forms of pressure', including pressure of economic or political character. This question was answered in the

negative, and thereby is 'the use of force' not including economic or political pressure on a state. In the same period, the UN general assembly indicated that the term "force" was not "coterminous with the term "armed force" and thereby strengthening the significance of the absence of the term "armed" in Article 2(4) of the Charter (Schmitt, 2011, p.575).

In the *Nicaragua* case, the ICJ expressly identified that certain actions that are non-kinetic in nature, can count as use of force (Schmitt, 2011, p.575). By this, the ICJ determined that a use of force can embrace acts that falls short of 'armed force'. Thereby, as noted by Schmitt (2011), non-physically destructive cyber operations could potentially fall within this term's ambit (p.576). In this respect, the threshold for a use of force "must lie somewhere along the continuum between economic and political coercion on the one hand and acts which cause physical harm on the other", according to Schmitt (2011). Hence, under Article 2(4) of the UN charter, states that initiate a cyber-operation might act on the threshold of a use of force. This is also to be seen in the Tallinn Manual, where a cyber attack is defined as 'a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects' (Pascucci, 2017, p.443). In this respect, the Tallinn manual implies that 'acts of violence' as defined in Article 49(1) should not be interpreted limited to kinetic action and one should rather consider the nature of the effect caused by the act to determine whether an act reaches the threshold of an armed attack (Pascucci, 2017, p.443).

According to Nguyen (2013), a case that comes close to this is the cyber attack that was experienced by Estonia in 2007. As the country of Estonia was complete paralyzed in the digital realm, the attack was more than just 'inconvenient' for the Estonian population, whereas the emergency number was unavailable for more than an hour and government and banking websites were shut down (p.184). Building further on this regard, Remus (2011) analyses this attack with Schmitt's analysis on the use of force as touchstone. According to Remus (2011), if the attacks would reach the threshold of use of force in Schmitt's analysis, Estonia would be entitled to act in self-defense as well as all NATO members through the collective defense mechanism (p.184). However, the level of 'armed attack' was not reached due to the incapability of considering the non-material effects of cyber attacks as a form of harm within Article 2(4) (Haataja, 2017, p.6). The level of violence meant in this context, "requires some form of injury to human beings or damage to physical property" rather than disruptions to the functioning of non-material entities such as networks and websites (Haataja, 2017, p.6).

Considerably, cyber attacks are likely to be situated in a 'grey area' below the threshold of the laws that regulates armed conflict and might be appealing to nation-states that aim to exploit this opportunity in order to avoid war but 'show' their capabilities regarding cyber operations. Considering this kind of cyber attacks that fall below the threshold of an 'armed attack', Lucas Kello (2017) made notion of the state of 'unpeace', which refers to the fact that most offensive actions in cyberspace have been conducted in a grey zone between peace and war. It can be argued that cyber threats have no intrinsic capacity for violence, at least not at the scale of intensity and destruction that conventional weapons can potentially cause. However, Kello argues, that "these skepticisms fails to acknowledge the broader agenda of international security studies, which covers issues such as the protection of social, economic and political interests against state threats that fail to satisfy the rigid criteria of war" (Kello, 2017, p.75). In this sense, Kello (2017) indicates that nation states find themselves in a continuing state of 'unpeace' where frequent cyber attacks are launched, however solely create a chaotic and uncertain environment but are not damaging enough to constitute a war. These acts fall below the traditional threshold of war but potentially can cause damaging effects on the economy and society of a nation state. However not lethal yet, new threats to civilian use of the internet cause a persistent disruption of cyber space which can potentially have severe impact on the lives of civilians.

3.2.2 Cyber attacks in the jus in bello

As illustrated in the previous section, the *jus in bello* governs the employment of force of military and other armed actors in armed conflict, including "who and what may be targeted" (Schmitt, 2012, p.284). In the *jus in bello*, or the framework of IHL, the term 'attack' triggers a wide array of legal protections (Schmitt, 2012, p.284). These legal restrictions and prohibitions derive from the IHL principles which requires the parties in an armed conflict to "distinguish at all times between the civilian population and combatants, and between civilian objects and military objectives, and accordingly direct their operations only against military objectives" (Schmitt, 2012, p.284). As seen in the previous section, Article 51 of the first Additional Protocol on the Geneva Convention, prohibits military operations to be directed against civilians, civilian objects and other protected objects and persons and must be understood essentially as "a prohibition on *attacking* them" (Schmitt, 2012, p.284). In order to determine the lawfulness of a military operation, the question is raised whether a certain act qualifies as an 'attack'. Schmitt (2012) illustrates that the term 'act of violence' denotes physical forms and does not include 'non-physical means of psychological or economic

warfare' (p.290). As cyber attacks are not likely to directly involve the release of violent forces, the question is raised whether and when cyber operations qualify as attack under IHL including the application of its prohibitions and restrictions.

Nevertheless, as noted by Schmitt (2012), the presence or absence of violence is not the crux of the norms described above. This became clear in the beginning of the 20th century, when chemical and biological weapons were considered as an attack prohibited under international law. These forms of attacks were banned because "they were instrumentalities that caused particular harmful consequences that international humanitarian law sought to avoid" (Schmitt, 2012, p.290). In this regard, 'acts of violence' are merely seen as instrumentalities that potentially cause consequences which should be regulated by the law and treaties must "be interpreted in context and in light of object and purpose" (Schmitt, 2012, p.290). In other words, the prohibitions and restrictions on attacks are not merely determined by the violent nature of an act, but rather with the occurrence of 'harmful or violent *consequences*' caused by an act (Schmitt, 2012, p.290). In this sense, attacks could be redefined as operations that result in, death or injury of individuals or destruction or damage of objects (Schmitt, 2012, p.291). Schmitt (2012) illustrates the example of a cyber attack on a water treatment plant in order to contaminate drinking water, this might result in severe illness among civilians. Regarding destruction, Schmitt (2012) note that cyber attacks might not cause physical damage to objects, however cyber attacks can potentially 'break' an object which might cause in inoperability and in-functionality of an object or system (p.291). Hence, the object and purpose of the additional protocols, is to avoid those very consequences to the extent that is possible in light of military necessity.

Cyber operations become increasingly attractive means to target an opponent due to its accessibility and low costs, especially for a weaker state to strike at a technologically more advanced, and therefore more vulnerable, adversary state (Schmitt, 2011, p.102). By this, the question is raised whether cyber-operations comprise as 'armed conflict', used in the IHL body of law as described above? As argued by Schmitt (2011), any operations qualifying as attacks under IHL would, if directed at civilians or civilian objects, constitute violations of IHL and war crimes (p.103). When Schmitt (2011) applies this view to cyber-operations, the author argues that "any operation by or attributable to a state that results in damage to or destruction of objects or injury to death of individuals of another state would commence an international object" (p.103). Considering this, it will be problematic to classify cyber-operations that cause no damage or injury, but instead merely disruption, disorder or inconvenience (Schmitt, 2011,

p.103). Despite the lack of physical destruction, such operations might be serious because of significant interference with a state's economy, transportation system or other critical infrastructures (Schmitt, 2011, p.103). In this respect, non-destructive attacks that do not pose physical risk to individuals and objects can have severe consequences for society, yet, not qualified as an 'act of violence' in the sense of IHL.

3.3 The Principle of Proportionality in Military operations

The cyber domain plays a more visible role in offensive military operations which and will tend to play an increasing role in conflicts of war scenarios (Cole, 2019). As described in the previous section, one of the conditions of the principle of proportionality is that a decision on a military act should involve the weighing between the anticipated military advantage and the potential civilian losses that will result from the particular military act. This section will explore, how the principle of proportionality is understood from a military perspective and answers the sub question "How is the principle of proportionality established in military security perspectives?". This initial question must be addressed in order to adequately apply the principle of proportionality in determining if an attack can be considered as justifiable. The definition of military advantage given in Haque's (2016) article on the principle of proportionality and necessity in law states that a military advantage can be considered as "any consequence of an attack which directly enhances friendly military operations or hinders those of the enemy, such as disabling opposing combatants, destroying their equipment, denying them opportunities to attack, and creating opportunities to attack them" (p.16-17). As noted by Brown (1976), the term 'military advantage' can be considered by a 'case-by-case' approach or on a 'cumulative' approach. The former refers to the specific military objective of a particular action, whereas the latter refers to the cumulative manner in which the act will contribute to the overall strategic goals (Brown, 1976, p.141).

The latter approach has been defended by the argument that 'taking civilian lives now will save more lives later' (Brown, 1976, p.142). However, this approach is not preferred by policy makers since this standard is 'vague and elusive' due to the difficulty of assessing 'how an act prevented undesirable future events and of determining how serious the adverse consequences would have been' (Brown, 1976, p.142). In the preferred case-by-case approach, a military advantage must be concrete and direct, whereby the former refers to an advantage which is substantial and clearly identifiable and the latter refers to an advantage which is caused proximately without further intervening agency (Haque, 2016, p.17). As stated by Brown (1976), the most notable early example of the 'direct military advantage' test has been the

bombings of Nagasaki and Hiroshima by the United States in 1945 (p.141). The bombings, that caused immense damage on the Japanese territory and its war industry, were justified by American statement that the military advantage gained from the bombings was strong enough to let the Japanese promptly surrender, which eliminated the necessity of an Allied invasion of Japan which would have inflicted heavy casualties on both sides (Brown, 1976, p.141).

Perhaps obvious, though it must be noted that the 'military advantage' must solely be military in nature. In this respect, political, economic or other non-military benefits are not relevant for the determination of proportionality in military operations (Gillard, 2018, p.11). Additionally, the expected military advantage must be quantifiable and identifiable, and most importantly, directly flow from the attack. Thus, advantages that are merely speculative or hypothetical will not be included in military proportionality assessments (Gillard, 2018, p.11). Another aspect of the proportionality assessment in military operations is the timeframe within the anticipated military advantage is expected to occur. However, the timeframe is not determinative *per se*, as stated by Gillard (2018) "it can be relevant as a long period between an attack and the expected occurrence of the military advantage may decrease the likelihood of the advantage occurring" (p.11).

Since the principle of proportionality requires the balance between two divergent values, military advantage and civilian life, it is not simple to make an objective balance. However, there is also no mathematical formula to balance for instance the military advantage to be gained by destroying a civilian object with an amount of civilian lives (Henderson & Reece, 2018, p.542). Contrarily, the proportionality determination is based on the subjective assessment of a military commander in question. In particular, military commanders are not expected to judge on the basis of an *ex post facto* assessment of the actual loss of civilian life and/or damage to civilian property in the aftermath of an attack, but are required to make decisions on the available information at the time of the attack in order to weigh the expected civilian damage against the anticipated military advantage (Barber, 2010, p.477). In other words, a military commander must determine the proportionality rule from the standpoint of the conditions at the time of the attack, rather than with hindsight according to the actual unfolding events (Henderson & Reece, 2018, p.542). In addition, there are no numerical limitations on the permissible number of civilian casualties in balancing the military advantage anticipated by an armed attack. So, even extensive civilian casualties do not need to be 'excessive' in the light of concrete and direct military advantage anticipated (Henderson & Reece, 2018, p.542).

It is considered to be difficult to balance the anticipated military advantage with the expected impact on civilians and to determine to what extend "mid- to long-term consequences of the attack may be taken into account" (Barber, 2010, p.480). This question, whether long-term consequences of an attack could be taken into account in assessing proportionality, has been considered by the International Criminal Tribunal for the former Yugoslavia in *Prosecutor v Kupreskić*. In this case, the trial chamber stated that "even when attacks may not fall foul under the rule of proportionality, the cumulative effects of such attacks may be taken into account such as to render the attacks 'not in keeping with international law'" (Barber, 2010, p.480). In other words, when longer term civilian damage caused by an attack is expected, such damage should be taken into account in the proportionality assessment as well. This is of particular importance in determining the presence of proportionality in military cyber operations, as a cyber attack can be invisible for a long amount of time. Unlike kinetic attacks in the physical world, the effects of cyber operations that can remain invisible to the naked eye until severe damage has been made. Consequently, it becomes more difficult to determine what should be considered as proportional collateral damage in the context of cyber attacks. Therefore, it becomes all the more valuable to examine the application of IHL principles on the protection of civilians from the effects of military cyber operations.

3.4 The potential human costs in cyber operations

To support the aim of this research, examining the role of the principle of proportionality in military cyber operations, it is essential to obtain a comprehensive understanding of the potential human costs of cyber means in military operations. In other words, *from which potential threats* is the principle of proportionality *protecting civilians*? In order to understand the human costs in armed conflict, the question "who is a civilian in armed conflict?" should be answered. In international armed conflicts, a civilian is essentially any person who is not a member of a state's armed forces (Gillard, 2018, p.27). In this respect, only the members of states' armed forces are combatants and any other person is a civilian, who loses protection from direct attack solely if he or she takes direct part in hostilities (Gillard, 2018, p.27). Hence, solely the harm posed on this definition of civilians will amount to the potential humanitarian cost in cyber operations described in this section. The traditional concept of harm relates to physical harm in respect to medical injuries and damage to certain objects. According to the article on the taxonomy of cyber-harms in the Oxford journal of cyber security (2018), in cyberspace, types of harm can be divided into physical harm, economic harm, psychological harm, reputational harm and social harm (Agrafiotis et al., 2018, p.7). As this research is

focusing on the types of harm that are protected under the principle of proportionality as ascribed above, the following section will focus on the *physical* type of harm caused by cyber security attacks, since the other four types of harm do not yet fall under the proportionality requirement as established in IHL. Examples of physical harm caused by cyber attacks is illustrated by Agrafiotis et al. (2018) as "damage or unavailable systems; corrupted data files; exfiltration or theft of sensitive or customer data; bodily injury to employees or customers".

The ICRC (2018), published a comprehensive report on the potential human cost of cyber operations based on the belief that the use of cyber operations during armed conflict is a new reality in present-day cyber military operations and the use of them is likely to increase in the future (ICRC, 2018, p.3). The report is particularly focused on the potential risks of cyber operations that might cause death, physical damage, injury affect the delivery of essential services to the population, or affect the reliability of internet services (ICRC, 2018, p.5). The ICRC report distinguishes three areas of particular concern, in terms of the potential human cost of cyber operations. These areas can be considered as the potential target areas of belligerents by using new tools of cyber technologies in order to cause damage to the civilian population of a state. The three areas of concern that potentially can cause physical harm to civilians are (1) cyber attacks that may affect the delivery of health care, (2) cyber attacks against industrial control systems, including those used in critical civilian infrastructure and (3) cyber attacks that target the internet core that can potentially have systemic effects (ICRC, 2018, p.6). To give an example of the health sector as the first area, in February 2016, all computer systems of the Hollywood Presbyterian hospital were seized by a hacker who claimed 17.000 dollar to give back access to the hospital's systems. Consequently, doctors of the Presbyterian hospital were unable to access patient's medical histories and could not share medical scans, x-rays or any other medical tests and some of the hospital's patients had to be diverted to nearby hospitals (Sienko, 2016). The malware could spread easily and quickly through the hospital's computer systems due to very weak security infrastructure and the lack of available backup data (Sienko, 2016).

The healthcare sector is rapidly moving towards increased dependency towards interconnectivity and digitization to adequately deliver health care services. Besides hospital computers used for internal management and filing hospital patients, there are computers embedded in medical devices which are connected to the hospital's IT system as well. Once a medical device as such is hacked, it can potentially give a deadly shock to the patient (Smeets, 2018, p.103). The report implies that manufacturers of medical devices are likely to not take

cyber security into account in designing and developing technological products for the medical sector (ICRC, 2018, p.19). In case of biomedical devices such as pacemakers and insulin pumps, many advantages are offered by connectivity as well. For instance, doctors can immediately react to a patient's evolving health situation by changing the device's settings themselves. To enable this, biomedical devices are required to have a Bluetooth connection to connect with another device which poses serious vulnerabilities to certain cyber attacks that are able to reprogram the device to malfunction, which can cause a patient's death. Therefore, as human lives are at stake in the health-care sector, it is important to increase effective cyber threat resilience and recovery capabilities of hospitals. In fact, students of the University of South Alabama successfully killed a simulated human by turning off its pacemaker by hacking it (Koebler, 2015). As stated by the students "It's not just the pacemaker, we could have done it with an insulin pump, a number of things that would cause life-threatening injuries or death" (Koebler, 2015, par.6). However, despite these striking findings, it is important to note that it will be difficult to establish whether medical device fatalities were caused by technical malfunctioning or were the consequence of a cyber attack (ICRC, 2018, p.19).

The second area of concern posed by the ICRC are "cyber attacks that target critical civilian infrastructure or that may otherwise affect the delivery of essential services to the civilian population" (ICRC, 2018, p.23). An example occurred in October 2019, when Indian authorities publicly confirmed that the country's largest nuclear power plant was the victim of a cyber attack. The Kudankulam nuclear power plant was hacked using malware that was designed for data extraction (Findlay & White, 2019). No significant physical effects were caused by the cyber attacks on the nuclear power plants. As stated in the report written on the cyber-attack, due to India's densely populated nature, a meltdown of one of the Kudankulam nuclear power plant would be an unimaginable major disaster (Mallick, 2019, p.4). Industrial control systems increasingly face numerous cyber-security threats with varying degrees of potential loss, ranging from non-compliance to disruption of operations which could result in destruction of property and potential loss of human life (ICRC, 2018 p.6). As industrial control systems are used in sectors such as electrical power, transportation and manufacturing, the unavailability of critical infrastructure as such caused by major cyber attacks could result in severe damage including potential loss of lives (Maglaras et al., 2018). Generally speaking, industrial control systems are protected by complex mechanisms that guarantee the safety and reliability of the systems. For instance, electrical network grids have multiple power sources to avoid widespread effects when one of its parts is malfunctioning (ICRC, 2018, p.6). However,

cyber attacks on specific 'nodes' in the system might cause a significant impact that can have severe harmful consequences. A peculiar aspect of industrial control systems as objective of attacking, is that attackers did not seem to be interested in the infrastructure in particular but rather in the secondary harmful effects, on the civilian population for instance (ICRC, 2018, p.6). The harmful effects can be caused directly, when the malicious actor is taking over control and manipulates the industrial processes. Or indirectly, by taking over the control systems about the processes by reducing the ability to monitor the processes or interfering with safety systems (ICRC, 2018, p.23). Thereby, when the system is disabled for a long time, the attack may cause physical damage. A clear example of an attack as such is Stuxnet attack on the Iranian nuclear program, which will be discussed in the following sections of this research.

The third area of concern are cyber attacks on internet services that potentially can take down the proper functioning of internet-based systems. Due to the connectivity of the internet, a targeted cyber-attack on the banking sector always bears the risk of affecting other systems or networks such as healthcare network services. While this form of cyber attacks would not directly cause physical harm, serious consequences on the delivery of essential services might occur. For instance, the internal systems of a particular essential service provider will be at risk when they are designed to function only if connectivity with the internet is available. The repercussions of such attack can potentially cause serious harm, in case of emergency ambulance services for instance. The significant consequences of an emergency number outfall are experienced by more than 11 million people in April 2014, when a software coding error in the Colorado facility caused that over 6,600 emergency calls never reached the public safety answering points (Public Safety and Homeland Security Bureau, 2014, p.1).

In the examples given by Agrafiotis et al. (2018) and the ICRC report (2018), the consequences of cyber attacks in the physical realm are merely indirect, through malfunctioning of certain critical systems where humans depend on. As these threats are serious threats, however, to this point in time, there is no clearly documented case of a cyberwar attack which caused directly loss of life. Hence, the risk of human cost based on current observations does not appear to be extremely high in comparison with the destruction and suffering caused by armed conflicts conducted in traditional ways (ICRC, 2018). In fact, the ICRC report noted that the potential trigger for military actors to carry out cyber operations, could actually avoid civilian harm. For instance, 'graphite bombs' are developed to cause dysfunction to targeted electricity grids, however, using cyber means to disable electricity grids can be more precisely targeted and tailored than destructive kinetic means. In that respect, physical damage or civilian

harm caused by kinetic bombs can be avoided by the use of precisely targeted cyber operations (ICRC, 2018, p.36). This view is supported by the article of Smeets (2018), where the notion is made of 'bloodless war'. The notion of 'bloodless war' is built on two pillars. The first pillar notes that cyberwar might make the world less violent as battles will take place in the digital realm rather than in the physical world, "a digital Pearl Harbor would cost fewer lives than the attack 70 years ago" (Smeets, 2018, p.104). The second pillar on the bloodless conception of war rests on the attacker's 'casualty sensitivity' (Smeets, 2018, p.104). Since a cyber-warrior is located far away from the battleground, "it is hard to conceive how these individuals can suffer bodily harm during an offensive cyber operation" (Smeets, 2018, p.104). In this regard, cyber operations may have the ability to limit casualties on both sides and can be considered as a push factor for conducting military operations that use cyber means and methods.

This view is supported by Carr (2010) who stated, "Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood" (p.2). However, despite the assumed advantages of a 'bloodless' war, Schreier (2015) states that it is unlikely that there will ever be a pure cyberwar that is fought exclusively in cyberspace with cyber weapons (p.28). Future wars will rather involve a mixture of conventional or kinetic weapons with cyber weaponry "acting as a disrupter or force multiplier" (Schreier, 2015, p.28). There is no strategic reason why an aggressor would limit itself to conventional weaponry, especially because cyber weapons has the ability to pose serious physical damage in a relatively precise and low-cost way (Schreier, 2015, p.28). As the ICRC report states, observed cyber threats are evolving faster than anticipated, in particular the threats regarding attacks against industrial systems (ICRC, 2018, p.8). Hence, with regard to the rapidly changing evolution of the use of cyber technologies in military operations, this development deserves close attention in order to examine the potential effects on human suffering (ICRC, 2018, p.8).

4. Case Study Analysis

4.1 The Stuxnet Attack

4.1.1 Geopolitical framework of the Stuxnet Attack

Stuxnet is considered as the first politically motivated cyber attack that was able to cause significant physical damage to a critical infrastructure facility of a nation state (Lenday, 2016, p.4). In order to understand the Stuxnet case in the context of proportionality in military cyber operations properly, it is valuable to briefly elaborate on the geopolitical context in which the

attack found place. The 'political motivation' related to the Stuxnet attack, should be viewed in the context of the concerns of the international community on the intentions and purposes of Iran's nuclear program. As Marr (2019) states it, "this unconventional strike hatched amid growing tensions between Middle Eastern Israeli and Palestinian actors in the long fought cat-and-mouse game to prevent Iran from attaining nuclear armament capabilities" (p.4). The Tehran Nuclear Research Center was founded in 1967 and was supplied with a nuclear research reactor from the United States which was known as the Tehran Research Reactor and consumed high enriched uranium as fuel source (Lee, 2012, p.3). To receive US nuclear support, Iran agreed on ratifying the Nuclear Non-proliferation Treaty (NPT) and thereby accepted the comprehensive safeguard agreement of the International Atomic Energy Agency (IAEA) (Lenday, 2016, p.4). These agreements were signed by Shah Mohammad who aimed to further expand Iran's nuclear program by building various nuclear power stations with support of the US President Eisenhower's Atoms for Peace program and several European countries (Bruno, 2010). With Western support, the nuclear program was steadily progressing through the early 1970s, however, a key turning point in the Iranian nuclear program occurred in 1979 (Bruno, 2010).

As a consequence of the Iranian Revolution, the last monarch of the country, Shah Mohammad, was replaced by the conservative Ayatollah Khomeini who declared the country to be an Islamic Republic. Hereafter, relations with Western countries were merely interrupted and, consequently, Western assistance was withdrawn from the development of the Iranian nuclear program (De Falco, 2012, p.38). In 1995, the nuclear program was restarted with an agreement between Tehran and Moscow for the re-construction of the Bushehr nuclear plant which was bombed and destroyed during the war with Iraq (1980-1988) (De Falco, 2012, p.38). According to De Falco, the great support given by Russia in reconstructing the Bushehr nuclear power plant, can be interpreted as an attempt to "re-establish an effective political influence in the Near-Eastern region that was lost following the collapse of the Soviet Union" (2012, p.39). In addition, tension between Western countries and Iran increased in 2002 when the IAEA conducted a three-year investigation program on Iran's nuclear activities and concluded that some of these activities had violated the safeguards agreement of the NPT and IAEA on nuclear weapons (Kerr, 2012, p.1). The gas centrifuges in Tehran produce high enriched uranium which is used in the production of nuclear weaponry. Subsequently, Iran's nuclear program generated widespread concern that the country's ambitions were beyond peaceful intent and thereby did not live up to its commitments to international obligations on nuclear weapons (Bruno, 2012,

p.8). Iran's response to the international skepticism on the country's intentions consists of consistent denial and claims that the uranium enrichment process is carried out solely for peaceful purposes (De Falco, 2012, p.42) (Bruno, 2010, p.1). Despite the skepticism and the continuous attempts of the international community to increase collaboration, Iran continues to develop its nuclear program.

Nevertheless, various violent attempts to stop or slow down the Iranian nuclear program were made by other means than cyber attacks throughout the past decennia such as assassinations of Iranian nuclear scientists, explosions and several bombings targeting nuclear facilities (De Falco, 2012, p.41). The Iranian regime has repeatedly accused the US and Israel of most of the described attacks "where the US has always strongly denied its involvement and Israel has held a more ambiguous position, refusing to officially comment" (De Falco, 2012, p.41) (Lee, 2012, p.24). Although no nation-state or organization have claimed the attack on the Iranian uranium facilities, there are various pieces of evidence that are pointing to the US and Israel as creators of the Stuxnet worm (Lee, 2012, p.23). According to recent exposed information, the Dutch intelligence agency AIVD has had a crucial role in the deployment of the Stuxnet attack by recruiting an Iranian insider that supposedly insert the infected USB into the systems of Natanz' facility (Zetter & Modderkolk, 2019). However, to date, neither the AIVD nor the CIA responded to these inquiries. As it is beyond the scope of this research to elaborate further on the attribution difficulties relating to the Stuxnet attack, this research will consider the US and Israel as the supposed creators of Stuxnet for the sake of the analysis. However important details about the Stuxnet attack remains speculative to date and is attributed to a particular actor yet, the Stuxnet case raised severe concerns about the possibilities on the use of cyber tools in military operations in the conduct of war.

4.1.2 How did the Stuxnet worm change the field of cyber warfare?

Although various forms of new malware appear daily, most of these are evolutionary variants of existing malware forms and don't have widespread impact on the global digital security landscape (Chen & Abu-Nimeh, 2011, p.91). However, in July 2010, the Stuxnet worm triggered the security community to learn new lessons by its complexity and unprecedented ability to damage industrial control systems (Chen & Abu-Nimeh, 2011). Whereas the Stuxnet attack shows remarkably detailed knowledge on the targeted industrial control systems, Stuxnet's creators of must have had in-depth knowledge of the targeted Iranian nuclear facilities during the preparation of the attack. In fact, the worm was designed in a way that it could properly operate autonomously, without any guidance from a command and control network at

distance (Lee, 2012, p.9). As this type of information on specific industrial control systems is not openly published, it can be assumed that the creators of Stuxnet have had insider knowledge on the Iranian facility, or derived information on the nuclear facilities with another cyber asset (Lee, 2012, p.9). The Stuxnet worm is considered by computer security experts as a game changer in the field of cyber security, described as "the most technologically sophisticated malicious program developed for a targeted attack to date" and as "a precision, military grade cyber missile" (Lindsay, 2013, p.366).

More significantly, due to the worm's unprecedented capability to result in the destruction of physical infrastructure, the Stuxnet worm is considered as "the birth of cyber-kinetic weapons" that opens the door to cyber attacks that can cause widespread disruption to civilian populations (Ivezic, 2018, par.2). Until Stuxnet, a significant feature of cyber weapons is their non-physical appearance, the effects of prior cyber attacks remained within the digital realm. Unlike any malware ever before, the Stuxnet worm could cause real-world, physical damage to its targets (Jenkins, 2013, p.69). As stated by Knapp & Langill (2015), prior to the Stuxnet attack, "it was believed that industrial systems were either immune or not being targets of cyber attacks" (p.50). This changed when it came to light that the Stuxnet worm was designed to target Iranian gas centrifuges in the city of Natanz' uranium enrichment program (Foltz, 2012, p.14). By its capability to make uranium enrichment centrifuges spin faster than they were supposed to, the Stuxnet worm causing the centrifuges to get out of control to the point of damaging the centrifuges. As put by Fruhlinger, as a result of the development of the Stuxnet worm "the world is a place where code can destroy machinery and stop or start a war" (2017)

The Stuxnet worm seemed to be designed to force a change in the facility's centrifuge's speed level by raising and lowering it continuously (Sanger, 2012). Due to the ability to manipulate the speed level, the Stuxnet worm caused to crack more than a thousand Iranian centrifuges which is suggested to sets back Iran's nuclear program back by several years (Foltz, 2012, p.14). In particular, the worm targeted the software used in programmable logic controllers (PLCs) to physical equipment such as pumps, delves and motors that run a specific program to control the speed of the Iranian centrifuges. The worm specifically targeted PLCs manufactured by the German company of Siemens in order to manipulate the speed of the centrifuges (Foltz, 2012). Unlike the majority of known malware, the Stuxnet worm was not designed to be spread via the internet but by the use of intermediary devices such as USB sticks (Farwell & Rohozinski, 2011, p.24). In this sense, the Stuxnet worm was able to target 'air-gapped' control systems, which means that the targeted systems were not connected to the

public Internet and infiltration required the use of intermediary devices such as USB sticks in order to gain access to the systems (Farwell & Rohozinski, 2011, p.24). In this regard, it was necessary to physically get the infected thumb drives onto laptop systems of personnel who were able to access the targeted facility. To date, it is unknown whether the initial infection was caused by an infected thumb drive that was used by an unknowing participant or implanted on purpose by a double agent instead (Lee, 2012, p.10).

Furthermore, the Stuxnet worm was very selective on its targets and was hunting for something in particular unlike other well-known malware that mostly infect every computer that it came across. Instead, when the worm entered a system it would proceed several checks and scans to determine whether the system was a targeted system. If it failed the checks, the attack was not implemented on that particular computer system. By this, the Stuxnet worm can be considered as an extremely selective malware whereas 'common' malware tends to be allegedly indiscriminate to the nature of systems that it comes across. Another unprecedented feature of the Stuxnet worm is the presence of four *zero-day vulnerabilities*, which is an unusually high number of unpatched vulnerabilities (Chen & Abu-Nimeh, 2011, p.92). With the use of *zero-day vulnerabilities*, a piece of malware is enabled to tackle previously unknown flaws in software programs or operating systems that create specific security weaknesses. In this regard, there is no time, 'zero-days', to develop and distribute patches to protect and fix the software flaws. The fact that the Stuxnet worm contained four zero-days vulnerabilities in its code, can be considered as an unprecedented number of unpatched vulnerabilities used in a piece of malware which illustrates the extraordinary level of sophistication and of the Stuxnet attack (O'Murchu, 2010, par. 4). Hence, the illustrated features of the Stuxnet worm pleads for its importance in the evolution of computer warfare and the capability of cyber-tools to cause physical damage, that could have severe consequences on civilians in times of war.

4.1.3 The principle of proportionality in the Stuxnet case, from a Jus ad bellum perspective

This section will provide an analysis whether the military cyber operation of Stuxnet in itself can be justified according to the *jus ad bellum* and *just in bello* proportionality requirements. As described in the previous chapters, the *jus ad bellum* provides certain criteria that determines morally permissible reasons for going to war. Stuxnet could be determined as a use of force due to its destructive effects on the nuclear facilities in a similar way as a bomb or missile might have, however its physical destruction was more limited and selective than a traditional bomb or missile would have caused. As the purpose of Stuxnet was to neutralize or set back the Iranian nuclear program, a kinetic strike would have been feasible as well to

physical destruct the nuclear facilities. However, by conducting Stuxnet, the United States and Israel were able to set back Iran's nuclear program using cyber force, causing not a single casualty or injury in the Iranian nuclear facilities. In this sense, this case insinuates a gray area of international regulations on the 'use of force' as laid down in Article 2(4) of the UN Charter. In this regard, the Stuxnet case generates a debate whether the attack represents a 'use of force' due to the physical damage caused to the nuclear facilities or as something less than the 'use of force', considering Stuxnet as a preferable 'non-violent' act in comparison with a possible kinetic airstrike against the Iranian nuclear program (Denning, 2012, p.677).

Nonetheless this debate can be considered as murky, it is not less valuable for future regulations on cyber weapons in military operations. In fact, whether the Stuxnet attack constitutes as a use of force is of significant importance in determining what responses would be justifiable under the IHL framework. The Stuxnet case is valuable for the future of cyber-warfare, as it can set a precedent for judging future cyber attacks that are able to directly cause physical damage outside the digital realm. As described in Chapter 3 of this research, the qualification of a cyber attack as a 'use of force' mostly depends upon the nature of the consequences of the attack. In other words, when cyber attacks cause physical damage to objects or injury to human beings, comparable with destruction caused in traditional warfare by kinetic attacks, cyber attacks can qualify as use of force.

The military objective of Stuxnet's creators to set back the Iranian nuclear program would be achieved as well by 'breaking' the nuclear facilities with kinetic force. For instance, by launching missiles on the Iranian nuclear facilities, the nuclear program would be severely delayed as well, caused by devastation. Nonetheless, a cyber-weapon was used which specifically targeted the systems of the Iranian nuclear facilities, without causing physical damage to the facility's surroundings and its personnel. In this regard, Stuxnet can be considered as a 'non-violent' alternative to possible military intervention of violent nature (Cristiano, 2018). Despite the Stuxnet attack had physical impact on the nuclear facilities, it must be considered as 'less physical', in any manner 'less lethal', than a destructive kinetic attack. According to Denning (2012), Stuxnet can be considered as a morally preferred action over a kinetic strike and potentially offer a gentler means of achieving a just military objective than through the use of lethal kinetic force (p.678). In this sense, the Stuxnet attack complies with the principle of proportionality in a *jus ad bellum* perspective, given that the cyber nature of the attack avoided excessive loss of civilian lives, injury to civilians or damage to civilian objects in relation to the direct military advantage anticipated.

As Article 2(4) allows for the use of force in two situations (1) when it is authorized by the UN Security Council under Chapter VII and (2) when the act is done in self-defense to an armed attack under Article 51 (Moore, 2015, p.8). According to publicly available information, at time of the Stuxnet attack, no imminent threat was posed by Iran on the use of enriched uranium to launch a nuclear attack on the US and Israel as alleged creators of Stuxnet (Marr, 2019, p.10). The concept of 'imminence' is described by the Chatham House principles on the use of force in self-defense as an instant and overwhelming threat which leaves no choice of means other than an act of self-defense (Willemshurst, 2006, p.967). Due to the lack of an imminent attack as such, or immediate aggression against the alleged creators of Stuxnet, Stuxnet cannot be considered as an act of preemptive or anticipatory self-defense.

In this sense, the Stuxnet case can be viewed in the context of preventive self-defense as the creators of Stuxnet attempted to delay or neutralize Iran's nuclear program in order to prevent a future nuclear threat. Preventive attacks are launched as an act of self-defense, in order to protect oneself from threats whereof it is yet unknown when and where the attack might occur (Potcovaru, 2017, par.7). In this regard, Stuxnet creators' ought to preventively halt Iran in achieving nuclear supremacy and future attacks that can be launched with such nuclear capacity (Marr, 2019, p.10). By this, the question raises whether a preventive action against the Iranian nuclear program was justifiable is questionable under the principle of proportionality. Although preventive acts of war are highly debated, in the article of Arquilla (1999), the author makes an argument for permissible preventive cyber attacks. The author claims that preventive attacks are questionable under the traditional Just War theory, however, "information warfare might prove useful in derailing the rise of a threatening power". In particular, cyber attacks that halt potential proliferation of weapons of mass destruction. As the Stuxnet attack is believed to be launched for similar purpose, advocates of Arquilla's claim can argue that Stuxnet is a justified preventive attack.

Although the instant effects of Stuxnet seemed to conform to the *jus ad bellum* principle of proportionality, considered to be 'non-violent' and even preferable in comparison to destructive kinetic attacks, attacks on nuclear power facilities are generally prohibited under the law of armed conflict. Article 56(1) of the first additional protocol to the Geneva Conventions grants special protection to installations containing dangerous forces, particularly to nuclear electrical generating stations, dams, dykes and other installations in order to avoid the release of dangerous forces that can cause severe losses among the civilian population (Dinniss, 2002, p.241). This article lays down the prohibition on the release of destructive forces

and grants special protection to the listed objects in order to protect severe collateral damage among the civilian population in times of war. Given the fact that Stuxnet destructed Natanz' and Bushehr's nuclear centrifuges, nuclear materials could have been released which certainly involves potential severe loss of civilian lives. However, Article 56 contains an additional clause which states that if a power plant provides "electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support" (van Engeland, 2011, p.65). By this, the prohibition on targeting nuclear power plants as laid down in Article 56 can be suspended when a nuclear power plant is not only used for commercial purposes but provides power for military objectives as well. Hence, if the Iranian nuclear facilities were indeed providing uranium enrichment for the development of military nuclear weapons, the Stuxnet attack would not violate Article 56(1) under IHL.

4.1.4 The proportionality principle in the Stuxnet case from a 'hypothetical' Jus in bello perspective

It is important to start this section with the notion that the law of armed conflict did not directly apply to Stuxnet because the US and Israel were not involved in an armed conflict with Iran at the time of the attack (Richmond, 2011, p.863). In this regard, the law of armed conflict cannot properly be applied on the Stuxnet attack, which solely applies during an armed conflict. In this regard, the Stuxnet attack can be viewed within the gray zone between peace and war as noted in Lucas Kello's argument of 'unpeace'. In the gray zone of 'unpeace', major powers are in a constant gray zone between war and peace by launching cyber attacks that fall under the threshold of the law of armed conflict, as described in the previous parts of this research. This section will elaborate on the Stuxnet cyber attack considered as part of a hypothetical war that is regulated under the law of armed conflict. It will be valuable to make such a hypothetical analysis as the Stuxnet worm is believed to be a precedent for cyber-kinetic weapons in the conduct of war to attack belligerents (Collins & McCombie, 2012, p.1). Scharre (2018) describes Stuxnet as an 'open source weapon', a weapon whose code is available online for other researchers to modify, fiddle with and repurpose for other attacks. Considering that the Stuxnet code is an 'open source weapon', future versions of Stuxnet are likely to be redesigned into even more advanced versions of the code before they will be launched. In this regard, Stuxnet can be considered as a blueprint for future cyber weapons and therefore valuable to examine in a *jus in bello* proportionality perspective.

Although the Stuxnet worm was never intended to spread beyond the Iranian nuclear facility at Natanz, the Stuxnet worm effected many computers around the globe beyond its

intended targets within Iran (Jensen, 2013, p.207). Due to an error in the code, the Stuxnet worm replicated and spread itself every time when an Iranian technician connected an infected laptop to the internet (Manzo, 2019). The effects that are caused by the Stuxnet malware to these computer systems might be a result of unintended infections. In other words, the effects to these computer systems can be considered as indirect effects of the Stuxnet attack. However, despite its exceptional capability to spread its infection rate, the Stuxnet worm did little or no harm to computers that are not involved in uranium enrichment. By this, the Stuxnet worm did not cause widespread damage because the worm was designed to affect Iranian uranium enrichment facilities only. As described above, the worm conducted certain checks to determine whether a computer is connected to specific PLCs manufactured by Siemens or not when it infects a computer system (Fruhlinger, 2017, par. 2). This is considered by Marr (2019) as "a noble attempt to plan for contingencies and protect innocent civilians from the destructive malware that the developers built" and significant prove that the developers of the Stuxnet worm "had no intent to hurt civilians" (p.11). In this view, Marr (2019) states that the Stuxnet developers show clear intent to protect civilians and avoid damaging anyone but the 'enemy' and sustain proportionality by the design of the Stuxnet code (p.11). In this regard, the *jus in bello* requirements of morality in war-time action have been upheld in the Stuxnet case if it was an attack that is regulated under the law of armed conflict.

Nonetheless, the Stuxnet worm eventually spread itself extensively in an unauthorized and unintended way, which implies that the worm could have cost severe harm to computer systems throughout the world if the worm was designed differently. In other words, without the above described 'checks' to determine whether the worm entered a system of Iranian enrichment facilities or not, the worm could have caused widespread damage to Iranian systems of critical civilian infrastructure. In fact, as the worm spread itself beyond Iranian borders to countries that has no part in this 'hypothetical armed conflict' governed under the *jus in bello* principles, non-participating countries could become victims of cyber attacks as easily as targeted countries. In other words, by using cyber means in war, the possibility of involving neutral countries in an armed conflict by, unintendedly attacking their national critical infrastructure, becomes a significant risk in military cyber operations. By this, the Stuxnet attack illustrates that the prosecution of cyber attacks and the effects of cyber weapons are both characterized with unpredictable collateral damage that can come with severe risks. For a fact, a kinetic airstrike on the nuclear facilities could cause collateral damage as well, when a nearby hospital is hit for instance. However, the Stuxnet case illustrates that by using a cyberweapon,

any hospital all over the globe could be affected as well by the attack due to its extensive spreading capability. Therefore, unpredictable outcome and effects of cyber weaponry are essential characteristics in analyzing the *jus in bello* principle of proportionality applied on cyber attacks conducted during military operations.

In war time, military commanders must anticipate on the unpredictable nature of cyber weapons when assessing the proportionality rule in order to protect civilians and civilian objects against the destructive effects of cyber attacks. This view is in line with Boylan's (2017) argument who states that in the context of traditional kinetic attacks, military commanders are well skilled and experienced in performing proportionality assessments on gathered intelligence on foreseen collateral damage by the use of traditional weapon systems (p.240). However, similar decision making may be difficult due to the nature of modern computer networks, which are able to operate across boundless distances in a speed which is "incomprehensible to the human mind" (Boylan, 2017, p.239). In this respect, military commanders should be supported by computer analysts in estimating collateral damage to civilians and civilian objects when determining the justifiability of a cyber attack under the rules of IHL. Nevertheless, as described in the previous chapter of this thesis, very few activities in cyber warfare will reach the threshold of an attack that will be conducted under the rules of IHL, thereby governed by the principle of proportionality.

As long as unclarity remains on the nature of cyber weapons in this regard, military commanders could use cyber attacks to pursue military goals without being subjected to the law of armed conflict, thereby the principle of proportionality in order to protect civilians. Cyber weapons as an alternative for kinetic weapons can be considered as an advantage due to the highly destructive character of kinetic weapons. As cyber-tools are developing rapidly into weapons that can potentially have severe consequences for civilians, a serious problem would arise when military commanders take advantage of the remaining unclarity on ruling and governing cyber weapons in order to pursue military goals without taking morality and the protection of civilians in consideration as established in IHL. In addition, as put by Smith (2019), governments not only perceive cyber weapon's as useful tools but also see them as "uniquely easy to use in a manner that evades detection" (p.118). In this sense, cyber weapons can be considered by governments as the 'perfect weapons' due to anonymity and the lack of certainty in the rules and principles that govern cyber-means of warfare.

4.2 The Israeli Defense Force – Hamas airstrike

4.2.1 Geopolitical framework of the IDF – Hamas airstrike

On the 5th of May 2019, the Israel Defense Forces conducted an airstrike on a Hamas facility that was allegedly housing an active Hamas hacking group, in operation to launch cyber attacks against Israel. Few days before the airstrike, violence between Israel and Gaza escalated to a degree that has not been seen in five years (Magal, 2019, par.1). Hamas launched more than six hundred rockets towards Israel, which responded immediately with approximately more than three hundred airstrikes on military targets in Gaza (Murphy, 2019). In response to an attempted cyber attack from Hamas, the IDF launched a targeted attack on the Gaza strip and destroyed the building which housed Hamas' cyber operations with kinetic force. As this event happened in an already full-fledged war, the airstrike must be analyzed within the context of an ongoing conflict where the power dynamic between the participating parties is already established (Murphy, 2019). For decades, there has been a continuous state of armed conflict between Israel and Hamas in Gaza on which the legal framework of international law of armed conflict applies as the conflict meets the definition of an 'armed conflict' as described in the *Tadic*[1] case (Israeli Ministry of Foreign affairs, 2009). Hamas is a highly organized and well-armed Palestinian Islamist political organization that has waged war on Israel since its founding in 1987 (Beauchamp, 2018). Given the fact that the Gaza Strip is neither a state nor an occupied territory by Israel, the armed conflict between Israel and Hamas is classified as non-international armed conflict in the current context (Israeli Ministry of Foreign Affairs, 2009). As stated in Israel's Ministry report (2009), this classification is of theoretical concern, as the norms and principles that govern both types of conflicts are merely similar in nature.

The digital realm is rapidly developing as a conflict area parallel to the physical military battlefield between Israel and Gaza. As stated by Shakarian & Ruef (2013), the armed conflict between Israel and Hamas illustrate how militants use cyber operations to support their information campaigns (p.41). A novel dimension of the battlefield is rapidly developed due to the ability to share digital images and messages from mobile phones to share information with the outside world on the conflict. As a result, cyber attacks became an attractive measure for both parties to support the war effort (Shakarian & Ruef, 2013, p.41). For instance, in 2017,

[1] In order to claim that the Israel – Hamas conflict meets the definition of an armed conflict according to the ICTY definition, the Israeli Ministry of Foreign Affairs report refers to the following decision in the *Tadic* case: "an armed conflict exist whenever 'there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State" (ICTY, 1999).

Hamas has built various fake applications to allure in Israeli soldiers' phones and steal sensitive security information from IDF soldiers. The IDF claims that Hamas cyber attackers used stolen identities to create social media profiles in order to attempt Israeli soldiers to download apps that would expose them to harmful malware that would allow Hamas militants to access personal information and control cameras and microphones on the smartphones (Perper, 2018, par. 3).

Before analyzing the IDF response to the Hamas cyber attack, it is important to note that Israel is not a party to Additional Protocol I, wherein the principle of proportionality is established in the IHL framework. However, the Israeli High Court of Justice (HCJ) has accepted the principle of proportionality as customary law, as dictated in the first Additional Protocol of the Geneva Convention (Hall, 2017, p.95). By this, the HCJ recognizes that IDF military commanders must adhere to the requirement of proportionality as established in IHL (Hall, 2017). In order to pursue this, the HCJ has adopted secondary tests to determine whether military actions are in compliance with the principle of proportionality which consist of (1) military actions or measures must lead to the actual realization of the military objective, (2) military actions or measures injure the civilian individual to the least extent possible and (3) the expected harm to the civilian population and civilian objects from those actions or measures must remain proportional to their beneficial gain (Hall, 2017, p.95). Although the principle of proportionality is recognized by the HCJ, the airstrike on Gaza's sole power plant whereby millions of civilians were cut off from electricity as referred to in the previous section is (Chapter 3.4) is an example of where the international community has raised questions about Israel's adherence to the proportionality requirement, as well as other core principles of IHL during armed conflicts.

4.2.2 How did the IDF – Hamas airstrike change the field of cyber warfare?

The significance of this airstrike lies in the fact that this is the first example of a military response to a cyber attack with an immediate kinetic attack that has been publicly attributed. Nevertheless, this was not the first time that a state that used kinetic force in response to cyber activities. In August 2015, for the first time a state used deadly force against hackers when ISIS hacker Junaid Hussain was killed by a targeted airstrike conducted by the US. However, the US airstrike on Junaid Hussain has been prepared for months in advance, while the IDF response to Hamas' attempt appears to be a response to "real-time war" (Murphy, 2019, par 3). In this regard, the airstrike can be seen as a critical moment in the evolution of the hybrid warfare between Israel and Hamas which involves both cyberattacks and kinetic fighting. This act is

another step in the ongoing debates on how cyber- and kinetic conflict should intersect with each other and how nations should create rules and norms to govern the new means and methods of conducting warfare. As stated by Murphy (2019), concerns were raised by this action in the international community due to the appearance that this airstrike "changed the rules of the game by permitting a state to respond with kinetic force to a cyber attack which had no direct physical ramifications" (par. 3).

It can be questioned whether this event could be the first step of a slippery slope whereby this airstrike could set a precedent that would allow an authoritarian nation to morally justify the use of kinetic lethal force in the physical realm, in response to cyber activity in the digital realm (Watson & Loomis, 2019, par. 4). Hence, on May 5th 2019, IDF used immediate severe kinetic force in response to an attempted cyber attack that caused severe destruction to civilians and civilian objects in the Gaza strip. Despite the alleged reason for the airstrike was unprecedented, it is important to note that the airstrike was part of a larger series of intense destructive actions between Hamas and Israeli militants that started a few days before the attack (Barth, 2019, par. 2). In the days before the airstrike, at least 27 people have been killed in the Israel-Gaza border area due to almost uninterrupted rocket fire from both sides (Tarnopolsky & Alouf, 2019, par. 1). The week wherein the airstrike occurred, has been marked as one of the largest escalations of fighting since the 2014 Gaza war, with more than 600 rockets been launched from Gaza into Israel and 320 airstrikes in response (Tarnopolsky & Alouf, 2019, par.1). As the airstrike was conducted amid a sharp increased violence in the Gaza strip, it can be questioned whether this airstrike is 'just another kinetic action in an armed conflict' or does this airstrike really 'cross a Rubicon'? It can be considered, that by this airstrike, a glimpse of future warfare is given where kinetic and cyber responses are increasingly used interchangeable (Groll, 2019, par 5).

The striking fact that the IDF chose to respond to the alleged cyber attack with the use of heavily lethal force while detailed information on the purpose or the technical attribution of the alleged cyber attack remains unknown for the public, raises questions on how cyber-kinetic responses may impact the protection of civilians during wartime. This event can be considered as a precedent for kinetic responses on cyber attacks to be a potential and acceptable measure during armed conflict, which also send out 'a message' to other state- or non-state actors that cyber attacks might be met by physical response. In this regard, civilians become increasingly vulnerable during armed conflicts as crucial information on the decision-making process of military commanders tend to remain unexplained due to the complexity and speed of cyber

attacks. Events of this sort impact the growing interconnectedness between the cyber domain and the physical world and undeniably rejects the assumption "what happens in cyber stays in cyber" (Vavra, 2019, par.3).

4.2.3 The principle of proportionality in the IDF – Hamas airstrike from a Jus in bello perspective

The airstrike poses new light on the question how to deal with cyber conflicts that spill over to the physical realm in times of armed conflict or war, regulated under the *jus in bello* principles and requirements of the Just War theory. This airstrike could set a precedent for nations to use lethal capabilities in response to cyber actions during armed conflicts. Therefore, it is valuable to examine this case in isolation, considering the effects of this event on the protection of civilians from the dangers arising from military operations in a cyber context. As described in the previous chapters of this research, when assessing the principle of proportionality, information on the expected incidental harm is crucial in order to balance the effects of the attack against the military objective that is sought. In this regard, this case will cover the question whether the IDF kinetic response on the targeted building is a proportionate one considering the military advantage anticipated from the attack. In other words, to assess the compliance with proportionality of this attack it should be determined whether the IDF kinetic response has been excessive in relation to Hamas' cyber-actions. However, The IDF did not release any detailed information of the nature of the Hamas cyber attacks that they were targeted with, other than describing the attacks as "a threat to the quality of life of Israeli citizens" (Ikeda, 2019, par 3). Harming the quality of Israeli citizens' lives could mean a broad range of things, from interrupting communication to attacking critical civilian infrastructures and hereby, the scope and purpose of the attempted cyber attack conducted by Hamas remains a black box. The lack of information on purpose and scope of the attempted cyber attack, makes it difficult to interpret the airstrike in a sense of morality and justice under the principles of IHL.

It is important to note that proportionality under *jus in bello* permits the use of traditional kinetic force against a cyber attack, as long as the effects of the attack are not excessive in relation to the anticipated military advantage (Dinniss, 2012, p.104). It can be argued that the airstrike conducted by the IDF can be justified as the Hamas hackers were allegedly carrying out an offensive operation on military behalf, engaged in armed conflict with Israel (Groll, 2019). As cyberspace is considered the newest domain of warfare, cyber-combatants can increasingly become targets of kinetic attacks as well as attacks in the digital realm, launched by non-state and state parties in an armed conflict. Nevertheless, when examining the

justification of this airstrike under the principle of proportionality, it is important to note that, however engaged in a persistent battle with Israel, these Hamas hackers were separated from the physical battlefield (Watson & Loomis, 2019). Therefore, it is arguable that these hackers were 'unarmed' combatants, threatening the 'quality' Israeli citizens' lives, although not posing a direct physical lethal threat to the lives of Israeli citizens in contrast to armed combatants in the fire line of the physical battlefield. Yet, the IDF decided upon to destroy the Hamas' cyberwarfare headquarter and thereby, kill the members of Hamas involved in cyber activities with lethal military force rather than a 'hack-back'. In this regard, it can be questioned whether the destructive airstrike on the targeted building has been excessive when weighing the anticipated military advantage. As the nature and scope of Hamas' cyber activities remains a black box, this question can only be answered by speculative arguments.

The airstrike seemed an immediate real-time response. However, due to the speed and lethality of the Israeli response, it can be assumed that the IDF already gathered detailed targeting intelligence and already recognized the potential threat coming from that building. Therefore, as stated by O'Flaherty (2019) it can be assumed that Israel had rather more information on the targeted building than cyber attack was launched from the building (par.4). The targeted building was known as the Al Ghussein building and was located in a densely populated civilian area, which is called the Al-Rimal neighborhood of Gaza (Humaid, 2019, par.1). The nature or purpose of an object is crucial in order to decide on the lawfulness of an airstrike under the *jus in bello* proportionality requirements of IHL. As laid down in Article (52) of AP I, objects that not qualify as military objectives must be considered as civilian objects (ICRC, 1977). Although little to no information on the specific purpose of the targeted building is publicly available, considering the Al Ghussein building was located in a civilian area, it can be questioned whether the targeted building was solely used as Hamas' cyber headquarters or was used as a civilian object as well. In other words, the legality of the airstrike depends on whether the Al Ghussein building was only effectively contributing to military action and thereby, not been used for civilian purposes such as housing.

According to publicly available information, the Al Ghussein building's main purpose was a base for the Hamas intelligence branch and their functions contributed effectively to military activities which makes the building a military object. In this sense, the IDF airstrike on the Hamas cyber headquarter can be considered lawful under the IHL regulations on targeting. Although in this case the targeted building seems to be a legitimate military object, this event raises questions in the debate on dual-use objects in the context of military cyber operations.

The fact that cyber attacks can be launched from computers that are located in every sort of building, which enables combatants to launch military cyber attacks even from their family residences, erodes the distinction between military- and civilian objects. In this sense, a family home can be considered as lawful military target due to the fact that it hosts effective military cyber activity. Hence, the number of objects that are simultaneously used for civilian- and military purposes is likely to increase. This development cause difficulties in determining whether damage is done to civilian parts of targeted buildings, which has strong impact on assessing the proportionality of an attack.

4.2.4 The proportionality principle in the IDF – Hamas airstrike from a 'hypothetical' Jus ad bellum perspective

As described in the previous section, the airstrike was not an isolated incident that occurred in peacetime and rather was part of a long-established armed conflict between two parties. This event can be considered as an indicative for future offensive 'deterrence-by-punishment' responses on cyber activities, with violent kinetic attacks that effects the physical realm (Murphy, 2019). Therefore, this sub-section will analyze this case in a hypothetical *jus ad bellum* perspective in addition to the previous section on the *jus in bello* in order to examine the consequences of this case on the protection of civilians from the use of cyber means in armed conflict. In order to determine compliance with the principle of proportionality of an act of self-defense, military commanders must take feasible precautions in the choice of means and methods of an attack to avoid excessive damage in relation to the anticipated military advantage. Nevertheless, states are not obliged to use similar means and methods to respond to an attack. In this regard, kinetic attacks could be responded by cyber actions and vice versa in compliance with the scale, scope, duration and intensity as required under the principle of proportionality. Accordingly, in the case of self-defense it needs to be determined whether the use of kinetic force is proportionate in relation to the use of cyber means in an armed conflict and vice versa. As put in the context of this case, it can be questioned whether or when a kinetic attack in response to a cyber attack, can be considered as proportionate use of force in order to neutralize the threat posed by Hamas.

Although the precise timeline is not given in public reports and media, it can be said that Hamas conducted its cyber attack around 9 a.m. local time on May 4th 2019 (Soesanto, 2019). The following day, at 5.55 p.m., the IDF announced on Twitter that they had successfully destroyed the allegedly Hamas cyber headquarters in the Gaza strip by an airstrike (Soesanto, 2019). By targeting the entire building, Israel instantly crippled Hamas' cyber capabilities in a

short amount of time, by using immediately military force to destroy Hamas' cyber capability during the active conflict. Hence, this instant response of the Israeli on the attempted cyber attack, allows the airstrike to be put in the temporal context of self-defense. Whether this airstrike can hypothetically be justified under the principle of self-defense established in the *jus ad bellum*, depends partly on whether the Hamas cyber attack can be considered as 'a use of force' that triggers Art 51 of the UN Charter on the right of self-defense as legitimate exception on the use of force as stated in Article 2(4) of the UN Charter. The former Article states that 'nothing in the Charter 'shall impair the inherent right of individual or collective self-defense if an armed attack occurs' (Dinniss, 2012, p.85).

As described in the previous chapters of this research, an 'armed attack' as laid down in the Charter could include a cyber attack directed against a State's critical infrastructure that can potentially cause social, political and economic stability for a prolonged period of time, - potential loss of life, - physical injuries or - damage to civilian objects (Gill & Ducheine, 2013, p.443). Put differently, cyber attacks could potentially fall within the realm of an 'armed attack' once the effects of the attack are similar to attacks conducted by kinetic force. However, in the case of IDF-Hamas, due to the lack of information on the scope and nature of the Hamas cyber attack it is futile to determine whether this cyber attack reach the threshold of 'armed conflict'. Nevertheless, for the sake of this hypothetical scenario, this section will consider the cyber attack as severe enough to reach the threshold of an armed attack. Although hypothetical, this research argues that it is valuable to examine the scenario of an armed attack by cyber means launched in peacetime under the *jus ad bellum* right to self-defense, as this is scenario can be considered inevitable for future wars due to the rapid military and technological development in the use of cyber means in warfare.

Considering the fact that the Hamas cyber attack has been encountered by the IDF before it could pose any harm to Israeli computer systems, in a hypothetical *jus ad bellum* scenario, this case can be viewed within the perspective of anticipatory self-defense (Soesanto, 2019). Acts that are regulated under the right of anticipatory self-defense imply that a targeted state may intercept an attack when the attack is imminent, rather than await the launch. Hence, anticipatory self-defense acts are responses to attacks that not happened yet, however there is significant proof that the aggressor state is in the final stage for launching the attack (Barnett, 2016, par. 18). The IDF announced on Twitter that the cyber attack has been stopped in the digital realm before the kinetic airstrike began. Spokesman from IDF, Ben Gen Ronen Malis, stated that after the bombing "Hamas has no cyber operational capabilities" anymore and "after

dealing with the cyber dimension, the Air Force dealt with it in the physical dimension" (Climpanu, 2019, par.2).

In this regard, the IDF intercept Hamas the cyber attack before the missiles were launched on the Hamas building. This means that the kinetic airstrike happened afterwards, in addition to the interception of the cyber attack in the cyber dimension. Considering that IDF intercepted and neutralized the cyber threat, and subsequently launched a kinetic attack on the Hamas' cyber headquarters, it is arguable that this case can be analyzed through the view of a preemptive self-defense act as well. The launch of a preemptive self-defense attack does not require a definitive or current threat, but rather the possibility of an imminent threat at some point in the future (DeWeese, 2015). In this regard, it can be argued that IDF launched a preemptive airstrike based on the belief that Hamas was about to attack again in the nearby future. As the airstrike allegedly destroyed and eliminated Hamas' cyber operation center, after the IDF intercepted the cyber attack it can be argued that Israel used a high level of kinetic violence to completely destroy Hamas' cyber operation capabilities. In this sense, however IDF neutralized the cyber-threat, the decision was made to launch the missiles that were bound to destroy the Hamas' building in order to counter the potential threat of cyber attacks at some point in the future (DeWeese, 2015, p. 86). Preemptive attacks as such pose severe difficulties in assessing the principle of proportionality as this form of attacks respond to acts that did not happen so far and therefore caused no physical damage to civilians or civilian objects yet. Especially in the context of cyber attacks, due to its unpredictable nature it is hard to anticipate on the expected physical damage that will be caused by the attack, thereby for the military commander to decide whether an attack is proportional in relation to the anticipated military advantage.

Conclusion

This research aimed to analyze how the principle of proportionality can protect civilians from the effects of military cyber operations. Based on qualitative literature analysis of recent studies on cyber warfare, this research has been built on the assumption that cyber attacks fall under the jurisdiction of international humanitarian law due to its potential destructive effects on civilians and civilian objects, similar to the effects caused by traditional kinetic force. As with attacks conducted by kinetic use of force, military commanders bear a responsibility to comply with the principle of proportionality when conducting an cyber-attack, in order to determine whether the expected incidental harm is excessive in relation to the anticipated

military advantage of an attack. However, deciding whether a cyber attack is expected to cause incidental loss of civilian life, damage to civilian objects, injury to civilians or a combination thereof in relation to the concrete and direct military advantage, is of utmost difficulty to determine in advance. Due to the unpredictable nature of cyber weapons, it is challenging to determine whether the effects of a cyber attack are excessive in relation to the military advantage. The analysis of the Stuxnet case illustrates that the global interconnected nature of the internet, poses severe challenges on the principle of proportionality in the context of military cyber operations. An important part of the proportionality assessment is the determination of the 'expected' collateral damage in relation to the anticipated military advantage. As seen in the Stuxnet case, due to an unforeseen error in the code and the worm's capability of extensive spreading, the virus infected numerous systems which were located all over the world.

In this sense, a cyber attack can cause severe collateral damage that even exceeds the boundaries of the targeted nation state in an armed conflict. Whether such collateral damage can be considered as an unjustifiable use of force according to the *jus ad bellum* requirements depends merely on the attack's effects on the victimized nation states. Even though there's no evidence yet of anyone losing their life directly caused by a cyber attack, does not mean that this scenario must be considered impossible. The potential human costs of cyber attacks become more realistic due to the rapid developing technology and the opportunities that created by increasing interconnectedness and society's digital dependency. Contrastingly, the Stuxnet case illustrated that cyber attacks can be considered 'preferable' in comparison with traditional kinetic force regarding collateral human costs of a military operation. In other words, as there is no evidence of a single lethal victim during the Stuxnet attack, it can be argued that cyber attacks give the opportunity to gain military advantage by the use of 'less-violent' means than kinetic force. However, it can be questioned whether the effects of future cyber weapons will remain less violent and preferable compared conventional notions of collateral damage or will future collateral effects of cyber attacks be unprecedented in scale due to the possibility of extensively spreading. It could be a matter of time when cyber attacks that affect the physical sphere will become the rule rather than the exception due to the speed of technological innovations.

Whether the direct effects of a cyber attack could be considered as an armed attack that triggers the right to self-defense, is crucial in determining whether a victimized state can invoke the right of self-defense. Although there is no exhaustive definition about what constitutes an armed attack in the UN Charter, it is accepted that the use of force is defined by the intensity of

the effects rather than by the nature of the used tool. It can be stated that due to the 'less lethal' nature of cyber attacks, the absence of physical damage to civilians or civilian objects, the threshold of an armed attack will less likely to be triggered. Consequently, a victimized state will not be justified to respond with armed force under the right of self-defense. The IDF-Hamas case demonstrated an unprecedented response to an attempted cyber attack by using destructive kinetic force. As the attempted cyber attack was intercepted by IDF before the airstrike, the kinetic response can be considered as a preventive act in order to destroy Hamas' cyber headquarters to protect Israel from cyber attacks in the future launched by Hamas 'just in case'. Therefore, the IDF-Hamas case presents a valuable possible *jus ad bellum* scenario where nation states act in advance to prevent future harm caused by attacks in the cyber realm. This scenario illustrates the demand for further elasticity of the principle of proportionality since preventive attacks makes it more difficult to determine whether an attack is proportionate to the military advantage anticipated as the military advantage that is gained by the attack is rather assumed speculative than based on an imminent threat. In this sense, it becomes harder to determine whether the military benefits of a preventive attack outweigh the harmful consequences that are possibly caused by the attack.

However, to date no cyber-attack reached the threshold of an 'armed attack' yet. This fact brings into question whether there is a shift between the *jus ad bellum* and the *jus in bello* towards a *jus in "Kello"*. The grey area illustrated by Lucas Kello (2015) seems to become of significant relevance in the context of using cyber tools in military operations. As illustrated, cyber attacks can potentially cause severe harm to civilians and civilian objects but are to date, 'non-violent' in nature. Therefore, it will be valuable to conduct further research on the role of the principle of proportionality in this 'grey area' between war and peace time. The ambiguous nature of cyber attacks leads to precarious questions when determining whether a cyber attack reach the threshold of an armed conflict. Although ambiguous, not less important to aim for more clarity on the application of traditional norms and regulations on the context of cyber attacks. Regarding the key role of the principle of proportionality, to protect civilians against excessive harm caused by attacks, it can be questioned whether this grey area can be considered as an optimistic or pessimistic state of being. On the one hand, to date, cyber attacks tend to be less violent and cause less excessive lethal harm than traditional kinetic force. On the other hand, by operating just below the threshold of an armed attack, nation states should be aware of a certain 'looseness' regarding the boundaries of the threshold of an armed attack which is challenged continuously. After how many attacks in the 'grey area' will a nation state 'lose its

temper' and seeks to strike back with use of force that actually reaches the threshold of an armed attack? Whether the proportionality requirement of a just cause could be meet in such scenario remains questionable due to the destructive nature of the response on 'grey area' attacks with a non-physical nature.

The focus of this thesis has been on military operations conducted by state actors being the key subjects of international humanitarian law. Therefore, it is yet to be questioned whether technology companies can be held accountable as subjects that are just as able as states to 'hit' in a cyberwar. Suppose that a technology company deploys a future increasingly destructive version of Stuxnet, is there a possibility that an act of war occurs between a tech company and a nation state? Who are the soldiers in this war and how can they be protected? It can be questioned what the role of IHL *will* be in a hypothetical scenario as such. Put differently, which body of law regulates tech companies when violating principles of the law of armed conflict and thereby be responsible for human suffering? As claimed by Kelly (2012) companies are already regulated by international law through economic frameworks and trade agreements, "the next step to bring companies under the ruling of international criminal law seems not a far stretch" (p.345). Considering the key role of technology companies in digital security concerns, they have supposedly a similar important role in protecting civilians from the effects of cyber attacks.

The rapidly expanding IoT and the 5G telecom networks will result in an even tighter internet-controlled connection between various systems used in offices, factories, transport systems and even in everyday devices in our homes. In this regard, network connections are increasingly become important elements of the future battlespace. By targeting a nation state's critical infrastructure, malicious actors are able to hit a nation's society straight in the core of providing vital services. As a consequence, besides the world's major powers, also minor ones are initiating to invest heavily in offensive and defensive military cyber capabilities. Due to the interconnected nature of digital networks, civilians and civilian objects are in a permanent state of vulnerability in the digital domain. A sphere that is accessible for anyone and is permanently in connection with everyone. In this sense, civilians are not only vulnerable for military operations when they are physically situated in an armed conflict. On the contrary, every civilian that makes use of international connected digital networks, can be affected by a cyber attack launched for military purposes. The development of these networks blurs the distinction between civilian and military systems to a large extent. In other words, agreement on the way

of treating network attacks in a similar way as conventional attacks using kinetic weapons, is essential in order to apply the framework of international law.

Another topic that further studies could address regarding the analysis of human suffering in the context of cyber warfare, is whether 'cognitive effects' such as confusion and disruption, can be considered as severe as physical effects on civilians and civilian objects of an attack? Is the world eventually turning into a place where physical losses have a similar impact to society as enduring disconnection to certain digitalized services, or even similar impact as physical losses? Cyber effects can concern anybody that use connected devices in daily life, whether that person lives in a peaceful or violate area of the world. Every civilian that owns network connected devices, can become a participant in war through increasingly growing networks between nation states. In this regard, the borders of war are become blurred and the institutes that protect civilians and their properties are challenged continuously as technology keeps developing rapidly. In fact, these borders are blurred to an extent that when two countries are in war, another country can become a victim of this war by unintended effects from a cyber attack that infected multiple computer systems throughout the globe such as Stuxnet. The question when and how to use cyber tools in military operations, and equally importantly how to regulate them, needs to be discussed and agreed upon at the global level by as many nation states as possible, in order to develop consensus on norms and agreement on the use of cyber weapons and how to respond proportionally to cyber threats. Both in real time as in proportional counterattacks and in preventive measures.

Reference List

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), tyy006.

Alexander, A. (2015). A short history of international humanitarian law. *European Journal of International Law, 26*(1), 109-138.

Avila, H. (2007). *Theory of legal principles*. Springer Science & Business Media. *81*, 1-5

Ayalew, Y. E. (2015). Cyber Warfare: A New Hullaballoo under International Humanitarian Law. *Beijing Law Review, 6,* 209-223

Barber, R. J. (2010). The proportionality equation: balancing military objectives with civilian lives in the armed conflict in Afghanistan. *Journal of Conflict & Security Law, 15(3),* 467-500.

Barnett, S. (2016, September 1). *Applying Jus Ad Bellum in Cyberspace*. E-International Relations Students. [Blog post] Retrieved from: https://www.e-ir.info/2016/09/01/applying-jus-ad-bellum-in-cyberspace/

Barnidge Jr, R. P. (2011). The principle of proportionality under international humanitarian law and operation cast lead. *New Battlefields/Old Laws,* 276-312.

Barth, B. (May 9, 2019), RiskSec 2019: Israel strike on Hamas hackers did not 'cross the Rubicon'. *SC magazine.* [Blog post]. Retrieved from: https://www.scmagazine.com/risksec-2019-philadelphia/risksec-2019-israel-strike-on-hamas-hackers-did-not-cross-the-rubicon/

Beard, J. M. (2018). The Principle of Proportionality in an Era of High Technology. *Oxford University Press, Lieber Institute for Law and Land Warfare Book Series-Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, edited by Christopher M. Ford and Winston S. Williams,* 1-23.

Beauchamp, Z. (2018, May 14). What is Hamas? Everything you need to know about Israel – Palestine. *Vox*. [Blog post] Retrieved from: https://www.vox.com/2018/11/20/18080058/israel-palestine-hamas

Boogaard, van den J. C. (2019). Proportionality in international humanitarian law.

Bruno, G. (2010). Iran's nuclear program. *Council on Foreign Relations, 10,* 1-8.

Cannizzaro, E. (2006). Contextualizing proportionality: jus ad bellum and jus in bello in the Lebanese war. *International Review of the Red Cross, 88*(864), 779-792.

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc.

Chen, T. and Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer. 44*(4), 91-93

Climpanu, C. (2019, May 5). In a first, Israel responds to Hamas Hackers with an air strike. *ZDNet.* [Blog post] Retrieved from: https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/

Cole, S. (2019). Cyberwarfare: Battlefield precursor for kinetic attacks? *Military embedded systems.* [Blog post]. Retrieved from: http://mil-embedded.com/articles/cyberwarfare-battlefield-precursor-for-kinetic-attacks/

Cristiano, F. (2018). From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. *Journal of War & Culture Studies, 11*(1), 22-37.

Cronin, B. (2013). Reckless endangerment warfare: Civilian casualties and the collateral damage exception in international humanitarian law. *Journal of peace research, 50(2)*, 175-187.

Dayem, L. (2018). The Ethics of Cyber Warfare. *The Illini Journal of International Security, 4*(1), 5-20.

De Falco, M. (2012). Stuxnet facts report: a technical and strategic analysis. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.*

Denning, D. E. (2012). Stuxnet: What has changed? *Future Internet, 4*(3), 672-687.

DeWeese, G. S. (2015). Anticipatory and Preemptive Self-defense in cyberspace: the challenge of Imminence. In 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. IEEE. 81-92.

Diamond, E. (2014). Applying International Humanitarian Law to Cyber Warfare. *Law and National Security: Selected*, (67).

Dinniss, H. H. (2012). *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University press.

Doffman. Z. (2019, May 6). Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. *Forbes.* [Blog post] Retrieved from: https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#4f37b89fafb5

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

Dunn Cavelty, M. (2012). The militarization of cyber security as a source of global tension. *Center for Security Studies.*

Durhin, N. (2016). Protecting civilians in urban areas: A military perspective on the application of international humanitarian law. *International Review of the Red Cross, 98*(901), 177-199.

Eichensehr, K. E. (2015). Cyberwar & International Law Step Zero. *Texas International Law Journal*, 50, 357.

Engle, E. (2012). The history of the general principle of proportionality: An overview. *Dartmouth* LJ, (*10)*1, 1-11.

Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. International Studies Perspectives, 17(3), 343-360.

Farwell, J. P. & Rohozinski, R. (2011) Stuxnet and the Future of CyberWar, Survival, 53(1), 23-40

Fenton III, H. A. (2018). Proportionality and Its Applicability in the Realm of Cyber attacks. *Duke J. Comparative & International Law, 29,* 335.

Findlay, S. & White, E. (2019, October 31). India confirms cyber attack on nuclear power plant. *Financial times.* Retrieved from: https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6

Forge, J. (2009). Proportionality, just war theory and weapons innovation. *Science and engineering ethics, 15*(1), 25-38.

Franck, T. M. (2008). On proportionality of countermeasures in international law. American Journal of International Law, 102(4), 715-767.

Fruhlinger, J. (2017, August 22). What is Stuxnet, who created it and how does it work? *CSO online.* Retrieved from: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Gatlan, S. (2016, May 6). Israel Bombs Building as Retaliation for Hamas Cyber Attack. *Bleeping Computer*. [Blog post] Retrieved from: https://www.bleepingcomputer.com/news/security/israel-bombs-building-as-retaliation-for-hamas-cyber attack/

Gill, T. D. (2015). International humanitarian law applied to cyber-warfare: Precautions, proportionality and the notion of 'attack'under the humanitarian law of armed conflict. *In Research Handbook on International Law and Cyberspace.* Edward Elgar Publishing.

Gill, T. D., & Ducheine, P. A. L. (2013). Anticipatory Self-Defense in the Cyber Context. *International Law Studies (Naval War College), 89*, 438-471

Gillard, E. C. (2018). *Proportionality in the conduct of hostilities: the incidental harm side of proportionality assessments.*

Gisel L. & Rodenhäuser T. (2019, November 28). "Cyber operations and international humanitarian law: five key points. *Humanitarian law & Policy*. [Blog post]. Retrieved from: https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/

Goodrich, P. (1984). The Modern Law Review, 47(5), 523-534

Groll, E. (2019, May 6). The Future is Here, and it features hackers getting bombed. *Foreign Policy*. [Blog post]. Retrieved from: https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology, 9(2),* 159-189.

Hall, C. W. (2017). To Throw a Stone in Palestine: The Principle of Proportionality and Children in the Israeli Military Justice System. *Denver Journal of International Law & Policy, 46,* 91.

Haque, A. A. (2013). Proportionality (in War). *International Encyclopedia of Ethics.*1-8

Haque, A. A. (2016). Necessity and Proportionality in the Law of War. *Cambridge Handbook on Just War (Larry May ed, CUP 2016*).

Henderson, I., & Reece, K. (2018). Proportionality under International Humanitarian Law: The Reasonable Military Commander Standard and Reverberating Effects. *Vanderbilt Journal Transnational Law, 51,* 835.

Huang, Z., & Mačák, K. (2017). Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. Chinese Journal of International Law, 16(2), 271-310.

Hurka, T. (2005). Proportionality in the Morality of War. *Philosophy & Public Affairs, 33*(1), 34-66.

ICRC (1977) *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* 8 June 1977, 1125 UNTS 3, Retrieved from: https://www.refworld.org/docid/3ae6b36b4.html

ICRC (2002). The Law of Armed Conflict. Conduct of operations – Part A. *Unit for relations with armed and security forces.* Retrieved from: https://www.icrc.org/en/doc/assets/files/other/law3_final.pdf

ICRC (2010): Development of modern international humanitarian law. Retrieved from: https://www.icrc.org/en/doc/who-we-are/history/since-1945/history-ihl/overview-development-modern-international-humanitarian-law.htm

ICRC (2013). *Cyber warfare and international humanitarian law: the ICRC's Position.* 1-4. Retrieved from: https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf

ICRC (2016). Report: The principle of proportionality in the rules governing the conduct of hostilities under international humanitarian law. *Université Laval*. Retrieved from: https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf

ICRC, Customary IHL Database, Retrieved from: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule42 on 16-12-2019

Ikeda, S. (2009, May 14). What Does Israel's Missile Strike on Hamas Hackers Mean for Military Cyber Response? *CPO Magazine.* [Blog post]. Retrieved from: https://www.cpomagazine.com/cyber-security/what-does-israels-missile-strike-on-hamas-hackers-mean-for-military-cyber-response/?

Jenkins, R. (2013). Is Stuxnet physical? Does it Matter? *Journal of Military Ethics, (12*,1), 68-79.

Jensen, E. T. (2012). Cyber attacks: Proportionality and precautions in attack, 198-2017.

Jørgensen, M. W., & Phillips, L. J. (2002). Discourse analysis as theory and method. Sage.

Kelly, M. J. (2012). Prosecuting corporations for genocide under international law. *Harvard Law Policy Review, 6*(2), 339-368

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kemp, J. (June 18, 2019). Massive Blackouts and the risk of cyberwarfare. *Reuters*. [Blog Post]. Retrieved from: https://www.reuters.com/article/uk-cyber-electricity-kemp/column-massive-blackouts-and-the-risk-of-cyberwarfare-idUKKCN1TJ1N8

Kerr, P. K. (2012). Iran's Nuclear Program: Tehran's Compliance with International Obligations. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Koebler, J. (2015, September 7). *Hackers killed a simulated human by turning off its pacemaker.* Vice. [Blog Post]. Retrieved from: https://www.vice.com/en_us/article/kbzmbz/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker

Kolb, R., & Hyde, R. (2008). Introduction to the International Law of Armed Conflicts. Basingstoke: Bloomsbury Publishing

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law, 23*(3), 220-237.

Kretzmer, D. (2013). The inherent right to self-defence and proportionality in jus ad bellum. *European Journal of International Law, 24*(1), 235-282.

Kubo Mačák. (2019) "This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace", ECIL Working Paper 2019/2.

Lee, R. M. (2012). The history of Stuxnet–Key takeaways for cyber decision makers. *Armed Forces Communications and Electronics Association (AFCEA).*

Lendvay, R. L. (2016). *Shadows of Stuxnet: recommendations for US policy on critical infrastructure cyber defense derived from the Stuxnet attack.* United States. CA Monterey: Naval Postgraduate school Monterey United States.

Lin, P., Allhoff, F., & Rowe, N. C. (2012). Is it Possible to Wage Just Cyberwar? *The Atlantic*. Retrieved from: https://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/

Lin, P., Allhoff, F., & Rowe, N. C. (2012). War 2.0: cyber weapons and ethics. *Communications of the. ACM, 55*(3), 24-26.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365-404.

Magal, P. (2019, May 10). "Israeli-Palestinian Conflict: Setting Precedents for Hacker Retaliation?" *Cyber series.* [Blog post] Retrieved from: https://www.cyberseries.io/newsroom/feature/israeli-palestinian-conflict-setting-precedents-for-hacker-retaliation/

Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., & Cruz, T. J. (2018). Cyber security of critical infrastructures. *Ict Express, 4*(1), 42-45.

Mallick, M. G. (2019). Cyber Attack on Kudankulan Nuclear Power plant. A wake-up Call. *Vivekananda International Foundation Paper.* New Delhi. Retrieved from: https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf

Manzo, V. (2013, January 29). Stuxnet and the Dangers of Cyberwar. *The inadvertent spread of the Stuxnet worm shows the need for transparent norms of digital conflict.* The National Interest. [Blog post]. Retrieved from: https://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030

Microsoft (30-03-2013) Five Principles of Shaping Cybersecurity Norms. [Blog Post]. Retrieved from: http://download.microsoft.com/download/b/f/0/bf05da49-7127-4c05-bfe8-0063dab88f72/five_principles_norms.pdf

Moore, A. (2015). Stuxnet and Article 2(4)'s Prohibition against the Use of Force: Customary Law and Potential Models. *Naval Law Review, 64*, 1-27

Murphy, M. (2019, June 24). What is the Threshold? Assessing Kinetic Responses to Cyber attacks. *Mad Scientist Laboratory*. [Blog Post]. Retrieved from: https://madsciblog.tradoc.army.mil/156-what-is-the-threshold-assessing-kinetic-responses-to-cyber attacks/

Newman, L.H. (2019, May 5). What Israel's Strike on Hamas Hackers means for cyberwar. *Wired*. [Blog Post] Retrieved from: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. *California Law Review, 101,* 1079.

Nolte, G. (2010). Thin or Thick? The Principle of Proportionality and International Humanitarian Law. *Law & Ethics of Human Rights, 4*(2), 245-255.

O'connell, M. E., Arimatsu, L., & Wilmshurst, E. (2012, May). Cyber security and international law. *International Law Meeting Summary, Chatham House*, 5-7.

O'Flaherty, K. (2019, 6 May). Israel Retaliates to A cyber attack with immediate physical action in a world first. *Forbes.* Retrieved from: https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber attack-with-immediate-physical-action-in-a-world-first/#48973e8af895

O'Murchu, L. (2010, 14 September). Stuxnet Using Three Additional Zero-Day vulnerabilities. *Symantec.* [Blog Post]. Retrieved from: https://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

Pascucci, P. (2017). Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution. *Minnesota Journal of International Law, 26,* 419-452.

Péguy, C., & de La Noue, F. (2002). Just wars, wars of aggression and international humanitarian law. *International Review of the Red Cross, (847),* 523-546.

Perper, R. (2018, June 14). "Hamas reportedly created a fake dating app to lure Israeli soldiers and steal security information". *Business Insider*. [Blog post]Retrieved from: https://www.businessinsider.nl/hamas-fake-dating-app-scam-israeli-soldiers-honeypot-glancelove-2018-7/

Petkis, S. (2016). Rethinking proportionality in the cyber context. *Georgetown Journal of International Law, 47*(4), 1431-1458.

Public Safety and Homeland Security Bureau. (2014). April 2014 Multistate 911 Outrage: Cause and Impact. (Public Safety Docket No. 14-72 PHSB Case File Nos. 14-CCR-0001-0007.). Retrieved from: https://docs.fcc.gov/public/attachments/DOC-330012A1.pdf

Quillin, W. J. (1926). REPORTS OF INTERNATIONAL ARBITRAL AWARDS RECUEIL DES SENTENCES ARBITRALES. *Cross-reference, 20*, 791-793.

Relia, S. (2016). *Cyber warfare: its implications on national security*. New Delhi: Vij Books India Pvt Ltd.

Remus, T. (2013). Cyber attacks and International Law of Armed Conflicts; a Jus ad Bellum Perspective. J. *International Commercial Law & Technology, 8*, 179-189.

Richmond, J. (2011). Evolving battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict. *Fordham International Law Journal, 35*, 842-896.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security, 49*, 70-94.

Roscini, M. (2010). Worldwide Warfare-'Jus Ad Bellum'and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, 14,* 85-130.

Sanger, E. (2012, June 1). "Obama Order Sped Up Wave of Cyberattacks Against Iran". *New York Times*. Retrieved from: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

Sanger, E., Barboza, D., Perlroth, N. (2013, February 18). Chinese Army Unit is Seen as Tied to Hacking Against U.S. *New York Times*. Retrieved from: https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Sari, A., & Tinkler, K. (2019). Collateral Damage and the Enemy. *British Yearbook of International Law.*

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war.* WW Norton & Company.

Schmitt, M. N. (2011). Cyber operations and the jud ad bellum revisited. *Villanova Law Review, 56(3)*, 569-606

Schmitt, M. N. (2011). Cyber operations and the jus in bello: key issues. *International Law Studies, 87(1),* 7.

Schmitt, M. N. (2012, June). "Attack" as a term of art in international law: The cyber operations context. *In 2012 4th International Conference on Cyber Conflict (CYCON 2012)*. 1-11. IEEE.

Schreier, F. (2015). *On cyberwarfare.* Geneva Centre for the Democratic Control of Armed Forces. 1-132.

Schulzke, M. (2017). *Just War Theory and Civilian Casualties: Protecting the Victims of War*. Cambridge University Press.

Sharkey, A. (2019). Autonomous weapons systems, killer robots and human dignity. *Ethics and Information Technology, 21(2),* 75-87.

Shaw, M. N. (2008). International Law 6ed. Cambridge University Press Textbooks., 1-10.

Singer, P. P. (2015). Stuxnet and its hidden lessons on the ethics of cyber weapons. *Case Western Reserve Journal of International Law, 47(1),* 79-86

Singer, T. (2019, May 22). Retaliatory Strikes as a Reaction to Cyber Attacks? *Völkerrechtsblog International law & International legal thought.* [Blog post]. Retrieved from: https://voelkerrechtsblog.org/retaliatory-strikes-as-a-reaction-to-cyber attacks/

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90-113.

Smit, B. (2019). *Tools and Weapons.* New York, NY: Penguin Press.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333-339.

Soesanto, S. (2019, May 8). Did Israel Have the Right to Bomb Hamas' Cyber HQ? *Defense One*. [Blog post]. Retrieved from: https://www.defenseone.com/ideas/2019/05/did-israel-have-right-bomb-hamas-cyber-hq/156829/

Steenberghe, R. van (2010). Proportionality under Jus ad Bellum and Jus in Bello. Common Features, Differences and Interconnections. In *Proportionality in Armed Conflicts*.

Sussman, R. H. (2017). The Resusable Bomb: Exploring How the Law of Armed Conflict Applies in Cyberspace. *BUJ Sci. & Tech. L., 23,* 481-521.

Taddeo, M. (2012, June). An analysis for a just cyber warfare. In 2012 4th international conference on cyber conflict (CYCON 2012) (pp. 1-10). IEEE.

"The Operation in Gaza, Factual and Legal Aspects", Report, Israeli Ministry of Foreign Affairs, July 2009, [Blog post]. Retrieved from: https://mfa.gov.il/MFA_Graphics/MFA%20Gallery/Documents/GazaOperation%20w%20Links.pdf

Tsagourias, N. (2012). Cyber attacks, self-defense and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229-244.

United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI. Retrieved from: https://www.refworld.org/docid/3ae6b3930.html [accessed 10 November 2019]

Van Engeland, A. (2011). *Civilian or Combatant? A Challenge for the 21st Century. Oxford University Press*, 65-67.

Vavra, S. (2019, May 6). "It was 'inevitable' that bombs would fall in response to a cyberattack". *Cyberscoop*. [Blog post]. Retrieved from: https://www.cyberscoop.com/hamas-cyberattack-israel-air-strikes/

Watson & Loomis (May 22, 2019). Crossing the cyber Rubicon: Views from both sides of the river. *Atlantic Council.* [Blog post]. Retrieved from:

https://www.atlanticcouncil.org/blogs/new-atlanticist/crossing-the-cyber-rubicon-views-from-both-sides-of-the-river/

Waxman, M. C. (2011). Cyber attacks and the use of force: Back to the future of article 2 (4). *Yale Journal of International Law, 36,* 421.

Wedermyer, L. J. (2012). The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict. Retrieved from: http://digitalcommons.law.msu.edu/king/241

Wilmshurst, E. (2006). The Chatham House principles of international law on the use of force in self-defense. *International & Comparative Law Quarterly*, *55*(4), 963-972.

Wood, M. (2013). International Law and the Use of Force: What Happens in Practice? *Indian journal of international law, 53*, 345-367.

Yates, J. A. (2013). *Cyber Warfare: An Evolution in Warfare not Just War Theory*. MARINE CORPS COMMAND AND STAFF COLL QUANTICO VA.

Zetter, K. (2014, March 11). An Unprecedented look at Stuxnet, the World's First Digital Weapon. *Wired.* [Blog post]. Retrieved from: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. & Modderkolk H. (2019, September 2). Revealed: How a secret Dutch mole aided Israeli Stuxnet cyber attack on Iran. *Yahoo News.* [Blog post] Retrieved from: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html

Zhuk, A. (2017). Does international human rights law impose constraints on digital manipulation or other cyberwarfare ruses? Analysis of the Stuxnet worm attack on Iranian nuclear facilities. *University of Chile*. Retrieved from: http://repositorio.uchile.cl/handle/2250/170163

Zollmann, J. (2016, October 2016). History as a Legal Argument – The Naulilaa Case (1928). [Blog post]. Retrieved from: https://lawlog.blog.wzb.eu/2016/10/28/history-as-a-legal-argument-the-naulilaa-case-1928/

Table of Cases

Case Concerning Oil Platforms, (Islamic Republic of Iran v. United States of America), 2003, Judgment, ICJ Reports 2003, p. 161.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, p. 14.

Prosecutor v. Kupreskić et al., (Judgment), Case nr. IT-95-16-T, Trial Chamber, 14 January 2000

Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999, Retrieved from: https://www.refworld.org/cases,ICTY,40277f504.html

Special Arbitral Tribunal, Naulilaa case, 31 July 1928, 2 RIAA 1011