

**Humanizing the law of cyber-targeting:**

**Human dignity, cyber-attacks and the protection of the civilian population.**

**By:**

Giacomo Biggio

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

The University of Sheffield

School of Law

December 2019

**Abstract.**

The main objective of my thesis is to argue whether a human dignity-oriented interpretation of the set of rules known as the ‘law of targeting’ can reduce the potential adverse effects related to the use of cyber technologies in times of armed conflict, thereby contributing to the process known as the ‘humanization of International Humanitarian Law’. In order to do so, I will discuss the process of humanization as being the result of the dynamic between the principles of military necessity and humanity, arguing for an interpretation of the principle of humanity grounded on the idea that the dignity of the individual must be respected even during wartime. I will then employ a human dignity-oriented interpretation to the notion of attack under Art. 49 of Additional Protocol I, in order to argue that the underlying notion of violence shall be interpreted more expansively and include, beyond cyber-operations causing physical violence, also cyber-operations causing serious psychological violence and serious economic violence. This would extend the definition of attack to a wider range of cyber operations, subjecting them to the rules of targeting and, by increasing the protection of the civilian population, would therefore enhance the process of humanization. Subsequently, I will discuss what are the major interpretive issues related to the application of the human dignity-based framework to the law of targeting in the cyber context, by examining the principle of distinction between civilians/civilian objects and combatants/military objectives, the principle of proportionality and the rules on precautions in attack and against the effects of attacks.

**Acknowledgments.**

At the end of this journey, I would like to thank all the people that helped me reach my destination. First and foremost, my supervisors, Professor Nicholas Tsagourias and Dr. Russell Buchan. I cannot thank you enough for the invaluable advice, support and patience that you have showed me throughout these years. Secondly, I would like to extent my gratitude to the Law School Staff for their work and professionalism, and I am especially thankful to Dr. Layla Skinns for her support. I would also like to mention my colleagues and friends: Andy Kastelic, Nota Kotzamani and Thekli Anastasiou, with whom I shared thought, doubts and laughter. Without you, this would have been a lonelier, less cheerful endeavour. Finally, and above all, I want to thank my family.

**Table of Contents.**

[Introduction. 9](#_Toc26944828)

[1.Cyber-attacks: definitions and relevance of the phenomenon. 9](#_Toc26944829)

[1.1. Distributed Denial of Service Attacks. 10](#_Toc26944830)

[1.2. Acts of cyber-sabotage directed against civilian infrastructures and private property. 11](#_Toc26944831)

[1.3. Ransomware attacks. 14](#_Toc26944832)

[1.4. Cyber-attacks in the context of military operations. 15](#_Toc26944833)

[1.5. The increasing relevance of cyber technology in international law. 16](#_Toc26944834)

[2. The ‘humanization’ of International Humanitarian Law 18](#_Toc26944835)

[2.1. Humanization and the creation of new IHL norms. 21](#_Toc26944836)

[2.2. Humanization of IHL and rule interpretation. 25](#_Toc26944837)

[3. Objective and structure of the thesis. 27](#_Toc26944838)

[4. Methodology and originality. 29](#_Toc26944839)

[Chapter 1. The relationship between the principle of military necessity and human dignity-based considerations within the law of targeting. Cyberwarfare’s interpretive challenges. 32](#_Toc26944840)

[1. The principle of Military Necessity and its functions in the *jus in bello*. 33](#_Toc26944841)

[1.1 Restrictive models of necessity: the use of lethal force under International Human Rights Law. 35](#_Toc26944842)

[1.1.i. Necessity under Article 6 ICCPR. 35](#_Toc26944843)

[1.1. ii. Necessity under Art. 2 ECHR. 37](#_Toc26944844)

[1.2. Restrictive models of necessity: the law on the use of force. 39](#_Toc26944845)

[1.2.i. Necessity under the jus ad bellum: the notion of ‘armed attack’ in its material and temporal elements. 41](#_Toc26944846)

[1.2. ii. Necessity under the jus ad bellum: the component of ‘last resort’*.* 43](#_Toc26944847)

[1.2.iii. Necessity under the jus ad bellum: the component of ‘immediacy’. 43](#_Toc26944848)

[1.3. The principle of military necessity and its functions. 44](#_Toc26944849)

[1.3. ii. Exceptional Military Necessity as a restrictive form of necessity in the jus in bello*.* 51](#_Toc26944850)

[1.4. Provisional Conclusion. 53](#_Toc26944851)

[2. Human Dignity and the foundations of the principle of humanity. 53](#_Toc26944852)

[2.1. Preliminary remarks. 53](#_Toc26944853)

[2.2. Human Dignity: Evolution of the idea, from Cicero to Kant. 56](#_Toc26944854)

[2.3. The contemporary meaning of human dignity. 59](#_Toc26944855)

[2.4. Human Dignity and the Limits to the applicability of Human Rights in times of armed conflict. 61](#_Toc26944856)

[3. The dynamic between the human dignity and military necessity within the law of targeting. 63](#_Toc26944857)

[3.1. The principle of distinction between civilians and combatants. 64](#_Toc26944858)

[3.1.i. The distinction between civilians and combatants. 65](#_Toc26944859)

[3.1.ii. The distinction between Military Objectives and Civilian objects. 68](#_Toc26944860)

[3.2.The Principle of Proportionality. 69](#_Toc26944861)

[3.3.The Rules on Precaution in Attack and against the effects of attack. 70](#_Toc26944862)

[3.4. The Principle of Unnecessary Suffering. 72](#_Toc26944863)

[4 .The emergence of cyberwarfare: challenges and opportunities for humanizing the law of targeting. 75](#_Toc26944864)

[Chapter 2. The notion of ‘attack’ in the cyber domain: towards a human dignity-oriented interpretation. 78](#_Toc26944865)

[1. The definition of attack under the *jus in bello*. 78](#_Toc26944866)

[2. The notion of Attack in the context of cyber operations: preliminary considerations. 81](#_Toc26944867)

[2.1. Cyber-attacks as physical violence: The Kinetic Equivalence Effect test. 83](#_Toc26944868)

[2.2. Alternative approaches to the KEE Test. 90](#_Toc26944869)

[2.2.i. The notion of ‘military operation’ as the main condition for the applicability of the rules of targeting. 90](#_Toc26944870)

[2.2.ii. The concepts of ‘capture, destruction and neutralization’ as qualifiers of an attack. 90](#_Toc26944871)

[3. Towards an Evolutionary interpretation of the notion of violence. 91](#_Toc26944872)

[3.1. The limits of reinterpreting ‘violence’ as including destruction of digital data. 94](#_Toc26944873)

[3.2. Psychological violence. 97](#_Toc26944874)

[3.3. Cyber-operations causing economic violence. 102](#_Toc26944875)

[4. Conclusion: cyber-violence and the need for a taxonomy of cyber-attacks. The role of Critical National Infrastructures. 105](#_Toc26944876)

[Chapter 3. The principle of distinction: civilians and combatants in the cyber domain. 108](#_Toc26944877)

[1. The Status of Combatant in Cyber Warfare. 110](#_Toc26944878)

[1.2. Requirements of distinction -Wearing a fixed distinctive emblem and carrying arms openly. 112](#_Toc26944879)

[1.2.i. Wearing a fixed distinctive emblem recognizable at a distance. 112](#_Toc26944880)

[1.2.ii. Carrying Arms Openly. 114](#_Toc26944881)

[1.3. Belonging to a party to the Conflict. 115](#_Toc26944882)

[1.4. Compliance with IHL. 119](#_Toc26944883)

[1.5. Members of a *levee’ en masse.* 119](#_Toc26944884)

[1.6. The requirements of lawful combatancy under Additional Protocol I. 121](#_Toc26944885)

[2. The notion of Direct Participation in Hostilities. 123](#_Toc26944886)

[2.1. Historical Evolution of DPH. The distinction between civilian and combatant and the lack of a treaty-based definition. 123](#_Toc26944887)

[2.1. The interpretive attempts precedent to the ICRC’s Interpretive Guidance. 127](#_Toc26944888)

[2.2 The ICRC Guidance on Direct Participation in Hostilities: its constitutive elements and their application to cyber warfare. 130](#_Toc26944889)

[2.1.i. Threshold of Harm. 131](#_Toc26944890)

[2.1.ii. Direct Causation. 134](#_Toc26944891)

[2.1.iii. Belligerent nexus. 138](#_Toc26944892)

[2.1.iv. The temporal scope of Direct Participation in Hostilities. 139](#_Toc26944893)

[3. Conclusion. 142](#_Toc26944894)

[Chapter 4. The distinction between civilian objects and military objectives in the cyber domain. 144](#_Toc26944895)

[2. Effective contribution to military action. 149](#_Toc26944896)

[2.1. War-sustaining function and war-fighting capabilities. 151](#_Toc26944897)

[2.3. The notion of effective contribution to military action in the cyber domain: concluding observations. 153](#_Toc26944898)

[3. The four criteria: Nature, Location, Use and Purpose. 154](#_Toc26944899)

[3.1. Nature. 154](#_Toc26944900)

[3.2. Location. 156](#_Toc26944901)

[3.3. Use and Purpose. 157](#_Toc26944902)

[4. Definite Military Advantage. 160](#_Toc26944903)

[5. Conclusion. 163](#_Toc26944905)

[Chapter 5. The Principle of Proportionality in Cyber Warfare and its applicative issues with regards to the relationship between the principles of military necessity and humanity. 165](#_Toc26944906)

[1. Evaluating Collateral Damage in the Cyber Domain. 168](#_Toc26944907)

[1.1. Applying the principle of proportionality in cyber: what kind damage counts in the proportionality assessment? 168](#_Toc26944908)

[1.2. The notion of ‘attack’ as a precondition for the application of the rules on proportionality. 170](#_Toc26944909)

[1.3 The notion of ‘incidental harm’ in the cyber context: are reverberating effects of cyber-attacks included in the proportionality analysis? 172](#_Toc26944910)

[1.4. What is ‘expected’ collateral damage in the cyber domain? 175](#_Toc26944911)

[1.5. The material scope of ‘expected’ incidental harm in the cyber domain. 179](#_Toc26944912)

[2. Military Advantage. 185](#_Toc26944913)

[3. Comparing collateral damage and military advantage in cyberspace: the meaning of the word ‘excessive’. 189](#_Toc26944914)

[4.Conclusion. 192](#_Toc26944915)

[CHAPTER 6 – The application of the principle of precaution in the cyber domain. 194](#_Toc26944916)

[1. Precautions in attack. 194](#_Toc26944917)

[1.1. Verification of military objectives. 196](#_Toc26944918)

[1.2. The obligation of minimizing collateral damage in the choice of means and methods of warfare. 200](#_Toc26944919)

[1.3. Precautions related to the principles of proportionality and distinction. 204](#_Toc26944920)

[1.4. The obligation to give effective advance warning. 206](#_Toc26944921)

[1.5. The obligation to choose the military objective the attack to which causes the least damage among civilians. 209](#_Toc26944922)

[2.Precautions against the effects of attacks. 211](#_Toc26944923)

[3.Conclusion. 214](#_Toc26944924)

[Concluding remarks. 216](#_Toc26944925)

[Bibliography. 222](#_Toc26944927)

[Journal Articles. 222](#_Toc26944928)

[Books. 228](#_Toc26944929)

[Chapters in Edited Volumes. 231](#_Toc26944930)

[Blogs, Magazines and Websites. 233](#_Toc26944931)

[Reports. 238](#_Toc26944932)

[Other national and international documents. 239](#_Toc26944933)

[National and International Cases. 239](#_Toc26944934)

[European Court of Human Rights. 239](#_Toc26944935)

[International Court of Justice. 240](#_Toc26944936)

[International Criminal Court. 240](#_Toc26944937)

[International Criminal Tribunal for the Former Yugoslavia. 240](#_Toc26944938)

[International Criminal Tribunal for Rwanda. 241](#_Toc26944939)

[Other National and International Cases 241](#_Toc26944940)

# Introduction.

The main objective of my thesis is to argue whether a human dignity-oriented interpretation of the set of rules known as the ‘law of targeting’ can have a positive impact on the employment of cyber technologies in times of armed conflict, thereby contributing to the process known as the ‘humanization of International Humanitarian Law’. In order to do so, I shall firstly introduce and define what cyber-attacks are and what is meant by the term ‘humanization of IHL’.

## 1. Cyber-attacks: definitions and relevance of the phenomenon.

Since the early 1980s, the popularization of the Personal Computer and the advent of the Internet have dramatically shaped the reality in which we live in. The rapid growth of information technology (IT) created cyberspace, a virtual domain which, according to the definition given by the US Department of Defense, consists in ‘the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controller.’ In the present day, digital information known as *data* travel in cyberspace, communicating instructions to computer networks and systems in order to operate nearly all services of vital importance for the functioning of modern societies, such as transportation, air traffic control, healthcare systems, water distribution and financial services. But great reliance on cybernetic technologies comes, however, with a greater risk of being subject by malicious cyber-attacks. In this regard, I will employ the terms ‘cyber-attacks’ or ‘Computer Network Attacks’ (‘CNAs’) to describe a specific category of computer network operations which, according to the definition given by the US *National Military Strategy* *for Cyberspace Operations*, consist in ‘[o]perations to disrupt, deny, degrade or destroy information resident on computers and computer networks, or the computer and networks themselves.’[[1]](#footnote-1) As such, CNAs employ tools known as ‘malware’, a category of various type of malicious programs designed to obtain unintended effects against the target computer network or systems. The past decades have seen CNAs increasing both in quantity and quality, going from data breaches and website intrusions engineered by teenage hackers in the mid-1990s to severely disruptive cyber-attacks, which took place both in peace time as well as in the context of an armed conflict. In this regard, while it not possible to provide the reader with an exhaustive list, I will nonetheless present a short catalogue of cyber-attacks methods and techniques, using real examples which will be scrutinised throughout different sections of my thesis. Furthermore, they will make the reader familiar with the different kind of cyberwarfare tools and techniques that may be employed.

### Distributed Denial of Service Attacks.

The first category of cyber-attacks I will examine are Distributed Denial of Service Attacks (hereinafter ‘DDoS’), a method of CNA that relies on the use of ‘botnets’ - that is, ‘infected’ computers operated by an user external from the owner – for the purpose of sending access requests to the IP of the designated target server.[[2]](#footnote-2) Eventually, the server is flooded with an extremely high number of such requests and eventually crashes. The most impactful DDoS attack to date (at least in terms of putting cyberwarfare on the map) happened against Estonia between the end of April and the beginning of May 2007.[[3]](#footnote-3) Following a controversy that arose between Russia and Estonia with regards to the relocation of the Bronze Soldier of Tallinn, a Soviet-era grave marker, on April 2007, a group of patriotic hackers (or ‘hacktivists’) called Nashi (‘Youth’) launched a coordinated DDoS attack against Estonian governmental and institutional websites and accounts, newspapers and broadcasters and banks and financial networks. The campaign of DDoS endured for no more than a week and caused no damage to physical infrastructure and civilians, nor did it result in significant financial losses. Yet, the incident increased the awareness on the potential adverse effects of cyberwarfare and prompted the establishment in the Estonian Capital of Tallinn of the NATO Cooperative Cyber Defence Center of Excellence (‘CCDOE’). While this attack took place in peace time, there have been a few instances DDoS attacks happened in the context of ongoing armed conflicts. Thus, during the armed conflict that took place during 2008 between Georgia and Russia, Russia launched a DDoS campaign which began on August 8, targeting governmental websites, which were also the object of ‘defacement’, since their visual appearance had been manipulated and displayed anti-Georgian propaganda.[[4]](#footnote-4) Particularly significant were the DDoS attacks against Israel in 2014 during the armed conflict against Hamas in the Gaza Strip, as they were carried out by Anonymous, a collective of ‘hacktivists’ without any unofficial or alleged State involvement. Thus, in July 2014 Anonymous released a YouTube video stating its intention to ‘wage a cyber-war against Israel’,[[5]](#footnote-5) which was then followed by the coordinated hacking of the accounts of senior State officials, the defacements of several institutional websites, including those of the Ministries of Education and Finance. More importantly, Anonymous launched a large-scale DDoS attack against the website of Prime Minister’s Office, the Ministry of Justice and those of the Israeli Defence Force (IDF) and Mossad, causing them to go offline.[[6]](#footnote-6)

### Acts of cyber-sabotage directed against civilian infrastructures and private property.

This category of CNAs targets civilian infrastructures and relies on highly sophisticated ‘viruses’ and ‘worms’ with high disruptive potential. These two types of malware infect the target system or network with self-replicating, malicious code which then spreads within the system, causing data disruption and alteration along its path. While a virus needs to be operated by an external user once it has entered a system, a worm is autonomous and does not need further human intervention.[[7]](#footnote-7) In this regard, the first instance in which a cyber-attack caused actual physical damage has occurred between 2009 and 2010, when the Supervisory Control and Data Acquisition Systems (SCADA) at the Iranian nuclear-enrichment plant of Natanz were targeted by what came to be known a Stuxnet.[[8]](#footnote-8) Stuxnet is highly complex computer worm that entered Natanz through USB drives, as the computer systems of the facility were ‘air gapped’ (not connected to the Internet). Once infiltrated, Stuxnet became scanning the digital environment searching for Siemens Step-7 software on PLC computers.[[9]](#footnote-9) The program laid dormant until these two conditions were met, then it propagated into the target computer systems, modifying the code and giving specific commands to the PLC. Thus, while one of the components of the worm manipulated the rotatory speed of the centrifuge, speeding them up or slowing them down, a second module hid all malicious files and processes, while also faking security certificates in order to prevent detection. Eventually, it has been estimated that Stuxnet caused the physical malfunction and destruction of thousands of turbines, reportedly setting back Iran’s nuclear weapons development programs by two years. [[10]](#footnote-10) Stuxnet remained the only cyber-attack to be known to have caused physical damage for several years, until 2014, when a cyber-attack directed against a steel mill in Germany caused physical damage by preventing a furnace from shutting down properly.[[11]](#footnote-11) Similarly, in July 2016, the Iranian oil industry was hit by a series of accidents which were allegedly caused by a cyber-operation. Thus, on July 6, a fire in the petrochemical plant of Bouali took three days to be extinguished and caused tens of millions of dollars in damages; less than two days later, a liquefied pipeline in the Marun Gas and Oil Production Company exploded, taking the life of a worker; then, on July 29 another fire broke down at the Bisotoon facilities in near the city of Kermanshah, lasting for two days.[[12]](#footnote-12) Significantly, the oil industry has been the target of the most economically disruptive CNA to date, when in August 2012 the discovery of the Shamoon virus was announced by private cybersecurity firms Symantec and Kaspersky Lab. The Shamoon virus successfully spread across the computer networks of the Saudi Arabia-owned oil company Saudi Aramco, erasing files on more than thirty thousand workstations for a time frame of a week, resulting in the manual replacements of the affected computer systems, delays in the distribution of oil and in financial losses of hundreds of millions in dollars.[[13]](#footnote-13) Although not as disruptive, similar versions of Shamoon have resurfaced in recent years, targeting the Italian oil firm Saipem in 2018, and the Electricity and Water Authority of Bahrain in August 2019.

A different, unprecedented kind of cyber-attacks, which has been firstly employed in the ongoing armed conflict between Russia and Ukraine, targeted the SCADA systems of electrical power grid in order to disrupt the provision of electricity and potentially cause physical damage. In this regard, there have been two documented instances so far. The first of these cyber-attacks was launched on December 13, 2005 and relied on a malware labelled ‘Black-Energy’ with which the attackers were able to infiltrate the SCADA systems of the three energy distribution companies operating in different provinces of Ukraine. Once the perpetrators gained control to the SCADA systems, they employed a malware known as ‘KillDisK ‘to erase data stored in servers and workstations. This disrupted the provision of electricity of the Ukrainian power grid which affected hundreds of thousands of people for several hours.[[14]](#footnote-14) Eventually, full operativity of the power grid was restored after several months. Then, between 17 and 18 December 2016, a more limited power outage took place in a power distribution station in Kiev, cutting off electricity supply for the Northern part of the city for an hour. Although the cyber-attack affected a relatively smaller area as compared to Black-Energy, the malware was employed was more sophisticated and potentially more disruptive.[[15]](#footnote-15) Identified as ‘Industroyer’or ‘CrashOverride’ by two cybersecurity companies, the malware was partly based on Stuxnet’s source code and performed similar functions.[[16]](#footnote-16) For instance, it could lay dormant waiting for its trigger condition to happen, it covered all its malicious files to prevent detection, could operate without human intervention and was designed to cause blackouts faster and on a greater scale compared to ‘Black-Energy’.

### Ransomware attacks.

A particularly worrisome kind of cyber-attacks are ransomwares, which are a category of malware that uses cryptography techniques to gain access to the victim personal data and/or block access to the target system. The perpetrator then threatens the victim of releasing the data or perpetually preventing them from using the system, unless they agree to the perpetrator’s conditions, which usually involve the payment of a ransom.

Which is exactly what happened in May 2017, when the WannaCry worm infected over 230,000 computers across more than 150 countries, particularly affecting Russia, Ukraine, India and Taiwan, and demanding payments of 300 $ in Bitcoin cryptocurrency within three days, and 600 dollars within seven days.[[17]](#footnote-17) More worryingly, WannaCry significantly affected the National Health Service (NHS) of the United Kingdom, causing the malfunction of over 70 thousand devices in England and Scotland, including MRI scanners and blood refrigerators.[[18]](#footnote-18) It was estimated that the ransomware attack caused economic losses for up to 4 billion dollars.
One month later, a variant of the ransomware ‘Petya’ (aptly named ‘NotPetya’) targeted companies and users primarily from Ukraine and Russia, while affecting also Italy, France, the US and the United Kingdom, causing estimated losses for than 10 billion dollars worldwide.[[19]](#footnote-19) Like WannaCry, NotPetya targeted, among others, two hospitals in the United States (in Pennsylvania and West Virginia), in what appears to be a wider trend in the target selection of ransomware attacks.

### Cyber-attacks in the context of military operations.

While many of the CNAs mentioned above happened in peace time, we can see an increase in the employment of cybernetic capabilities in the context of armed conflict too, albeit for different purposes and with different kind of cyber-attack techniques, essentially aimed at supporting conventional attacks.

Thus, during Operation Allied Force the US contemplated to launch a cyber-attack against Serbia’s air command network, to prevent it from targeting NATO aircraft. However, the CNA was called off due to possible adverse consequences on civilians and because its legality was questioned.[[20]](#footnote-20) The same method was also considered against the government of Ghaddafi during the 2011 armed conflict in Libya, although the attack was cancelled as it raised analogous concerns.[[21]](#footnote-21) Differently from the previous examples, a successful attempt has allegedly been made by Israel in 2007, when the targeting of a nuclear facility in Syria was facilitated by a cyber-attack that neutralized Syrian radar and anti-aircraft systems.[[22]](#footnote-22) Although not specifically related to the context of an ongoing armed conflict, the last documented instance of cyber-operation in the context of military operations, in June 2019, the United States Cyber Command hacked Iranian rocket and missile launch systems, in retaliation for the dawning of a U.S. Drone and attack on oil tankers in the State of Hormuz by Iran.[[23]](#footnote-23)

### The increasing relevance of cyber technology in international law.

It comes as no surprise, then, that cyber technologies became to be perceived as an important factor in the field of international security. This has been reflected in the development by States of cyber-related security strategies, the integration of cyber within their military doctrines, and the creation of cyber-related units in the ranks of their armies, such as the US Cyber Commands, China’s PLA Unit 61398, and IDF Unit 8200 among others. At the international level, the UN has addressed the emergence of cyber technology on various occasions, most importantly when in 2002 the UN General Assembly passed a resolution related to the ‘Development in the field of information and communication in the context of international security’ in which it requested the UN Secretary-General to establish a group of governmental experts (hereinafter ‘GGE’)to report on international concepts aimed at ‘strengthening the security of global information and communications systems.’[[24]](#footnote-24) Although eventually the first GGE did not submit any report, further GGEs were established by subsequent General Assembly Resolutions, agreeing over the fact that norms regulating cyberspace could be developed over time and that international law, especially the UN Charter and the principle of state sovereignty, does apply to cyberspace.[[25]](#footnote-25) However, the fourth GGE, which was established in December 2015 and was due to report in 2017, did not reach a consensus as to how, specifically, international law should apply.[[26]](#footnote-26) For instance, both China has been reluctant towards the application to cyberspace of International Humanitarian Law (IHL), as it would lead, in the opinion of their representatives, to a militarization of cyberspace.[[27]](#footnote-27)

The task has been recently taken on by academics, most notably by the Group of Experts (GoE) on invitation from the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), which resulted in the publications of the *Tallinn Manual of the International Law Applicable to Cyberwarfare* (‘Tallinn Manual 1.0’) in 2013,[[28]](#footnote-28) and *The Tallinn Manual 2.0 on the International Law applicable to cyber operations* in 2017.[[29]](#footnote-29) The two versions of the Manual focus*,* *inter alia*,on the application of the two branches of international law that regulate the use of violence in international relations, namely the law on the use of force (*jus ad bellum*) and International Humanitarian Law (*jus in bello*). While the law of use on force is concerned with limiting the recourse to armed violence by States in their international relations and is regulated by Art. 2.4. of the UN Charter, International Humanitarian Law (also known as the law of armed conflict or the *jus in bello*), applies from the moment there is an armed conflict within the territory of a State. In this regard, an armed conflict is defined as ‘a State of protracted armed violence’[[30]](#footnote-30) which can be qualified as international, if it takes place between States, or non-international, if it takes place ‘between a State and organized armed groups, or between such groups within a State.’[[31]](#footnote-31) Accordingly, the scope of my research is limited an analysis of cyber-operations taking place in the context of an armed conflict to which International Humanitarian Law Applies, a phenomenon that will be referred to as ‘cyberwarfare’. More specifically, I will be using the term to refer, firstly, to a scenario in which a State carries out cyber-operation against another State in the context of an international armed conflict. Furthermore, the term will be used to describe a scenario where, in the context of a non-international armed conflict, a cyber-operation is mounted by non-State actors which are under the control of a State - so that any cyber-attack of the former can be attributed to the latter under the law of State Responsibility – or which have pledged allegiance to a State. Delimiting the scope of my research to cyberwarfare operations excludes instances of cybercrime, a notion that describes cyber operations carried out by State or non-State actors where no such situation of armed conflict exists and, therefore, when International Humanitarian Law does not apply.

Having clarified this, my thesis will discuss to what extent the emergence of cyberwarfare can positively affect the application of the rules on targeting under IHL, and specifically on the process known as ‘humanization of international humanitarian law’, which I shall now introduce.

## 2. The ‘humanization’ of International Humanitarian Law: definition and scope of application of the concept.Writing more than one hundred years after the first Hague Convention was signed, Theodor Meron argued that the modernlaw of armed conflict had undergone a transformation which began in the aftermath of the Second World War, starting when the Geneva Conventions were drafted in 1949. Since then, the law of armed conflict has been progressively influenced by ideas aimed at increasing the protection of the civilian population – and, albeit to a lesser extent, safeguarding the lives of combatants – against the nefarious effects of warfare. The quintessential driver of this process, which he termed as the ‘humanization’ of international humanitarian law, has been the interaction between the principle of military necessity, which has been traditionally considered as the cornerstone of the law armed conflict, and the emergence of a ‘principle of humanity’,[[32]](#footnote-32) which has progressively eroded the scope of application of the principle of military necessity. The principle of humanity has been firstly referenced in the preamble of the 1899 Hague Convention, which declared that:

‘’Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established by the civilized nations, *from the laws of humanity*, and the requirements of the public conscience.”[[33]](#footnote-33)

A modernized version of the Preamble, better known as the Martens Clause, named after the Russian diplomat who proposed it, is found in the Geneva Conventions, where the ‘laws of humanity’ have been replaced with the words ‘principle of humanity’. It is now commonly understood that the term ‘principle of humanity’ is synonymous for ‘humanitarian considerations.’[[34]](#footnote-34)I will therefore employ these two terms interchangeably in the course of my thesis.

The relevance of humanitarian considerations within IHL has been long recognized by International Courts and Tribunals, beginning with the Corfu Channel case, where the ICJ argued that the obligation, incumbent on the Albanian government, to notify British warships of the existence of a minefield in its territorial waters, was not based on the Hague Convention of 1907, but rather on ‘elementary considerations of humanity, even more exacting in peace than war.’[[35]](#footnote-35) From then on, the importance of the principle of humanity has been reiterated on several occasions. Thus, in Nicaragua, the Court recognized that the rules specified in Common Article 3 of the Geneva Convention ‘constitute a minimum yardstick, in addition to the more elaborate rules which are also to apply to international conflicts; and they are rules which, in the Court’s opinion, reflect what the Court in 1949 called ‘elementary considerations of humanity.’[[36]](#footnote-36) Similarly, in its Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, the World Court affirmed the view that the rules of international humanitarian law were’ fundamental to the respect of the human person and elementary considerations of humanity.’[[37]](#footnote-37) The principle of humanity has been mentioned several times by the jurisprudence of the ICTY, in cases such as Kupreskic,[[38]](#footnote-38) Celebici,[[39]](#footnote-39) and Martic, where the Trial Chamber noted that the most important principles of the jus in bello emanated from the elementary considerations of humanity ‘which constitute the foundation of the entire body of international humanitarian law applicable to all armed conflicts.’[[40]](#footnote-40)

Significant as they may sound, the above statements do not shed any light with regards to the nature and the function of the principle of humanity within the *jus in bello*. Doctrinal views on the matter are also divided, between authors who elevate the principle to the rank of source of law, those who assign it the more limited role of ruling *a contrario* arguments on the inapplicability of IHL in areas not yet regulated by it, and finally those who consider the Martens Clause no more than a rhetorical gimmick employed to break a diplomatic impasse.[[41]](#footnote-41) While addressing each and every position over the nature of the principle of humanity is beyond the objective of my research, I will however contend with the one argument, made most notably by Yoram Dinstein, according to which the principle of humanity cannot be truly considered as a ‘principle’, since it is not integrated into positive rule and does not, in and of itself, give rise to any specific obligation. Thus, he argues that ‘there is no overarching, binding, norm of humanity that tells us what we must do (or not do) in wartime.’[[42]](#footnote-42) What we actually encounter are humanitarian considerations, which pave the road to the creation of legal norms and thus explain the evolution of IHL.’[[43]](#footnote-43) In this regard, I do not entirely agree with Dinstein’s view in the sense that I believe that ‘humanitarian considerations’ do actually operate as a principle within the normative framework of IHL. To better illustrate my point, an explanation of what I mean by the word ‘principle’ is necessary. A principle of law can be described as a proposition (or a set of propositions) that reflects the values of a particular order or community and translates in legal terms the normative and organizational principles of said order or community. Principles of law can be further distinguished between normative-ideational principles and structural-organizational principles. Normative-ideational principles are ‘the pivotal and archetypal principles of a particular order, its *creator spiritus* and *raison d’etre*’,[[44]](#footnote-44) providing unity, consistency and direction to the referent order.[[45]](#footnote-45) On the other hand, structural-organizational principles have the function of organising and managing the legal relations within a particular order, thus mediating between the normative-ideational principles (from which they are derived) and specific legal rules.[[46]](#footnote-46) Within IHL, the principle of humanity represents a normative-ideational principle, reflecting the values comprised within the notion of ‘human dignity’, a concept the meaning of which will be explained in greater detailed in Chapter 1. The principle of humanity, then, influences the norm-creation process of IHL as it is reflected into certain structural-organizational principles,[[47]](#footnote-47) which are then translated into specific legal rules. Beyond influencing the normative evolution of IHL, the principle of humanity also possesses the function of being an interpretive tool, whereby the rules of the *jus in bello* can be interpreted in a way that is consistent with the values expressed by said principles. I shall now examine these two functions in more detail.

### 2.1. Humanization and the creation of new IHL norms.

 Firstly, the principle of humanity propelled the codification of new rules of IHL in areas that were under-regulated, or outside the purview of the law. In this regard, the turning point has been the drafting of the Geneva Conventions in 1949 and their two Additional Protocols, in 1977, which can be considered a paradigmatic shift from a State-focused system to a humane-centred, individual rights- based legal regime. As Kolb observed, the normative framework that existed prior to 1949 was essentially concerned with limiting the use of certain types of weaponry, such as exploding bullets, asphyxiating gases, and weapons of a nature to cause superfluous injury or unnecessary suffering.[[48]](#footnote-48) The rationale behind these restrictions was rooted in the considerations that ‘the right of belligerent to adopt means of injuring the enemy is not unlimited’;[[49]](#footnote-49) as such, ‘the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy’,[[50]](#footnote-50) a task for which was deemed ‘sufficient to disable the greatest possible number of men.’[[51]](#footnote-51) These statements and proclamations, which are found in several of the early instruments of the modern *jus in bello*, are a testament to the fact that, at that time, States were already developing an interest in regulating warfare in an attempt to mitigate its consequences. However, while these rules can be seen as the consequences of a humanitarian sentiment that would later bloom into full effect, it must be however be pointed out that they were only limited to safeguarding the lives and security of combatants, while the figure of the ‘civilian’ remained undetected and outside the scope of the law of armed conflict. In contrast, the Geneva Conventions put the protection of the civilian population and civilian objects as their primary concern, by providing a detailed set of rules that would apply to international armed conflicts (what were traditionally understood as ‘inter-State wars’) to selected categories of ‘protected persons’, namely wounded and sick at land (GC I),[[52]](#footnote-52) wounded, sick and shipwrecked at sea ( GC II),[[53]](#footnote-53) prisoners of war (GC III),[[54]](#footnote-54) and most importantly to persons ‘not taking an active part in hostilities’ such as civilians, including the population of occupied territories ( GC IV).[[55]](#footnote-55) Furthermore, the protective scope of the Conventions was no more limited to international armed conflicts, which had been the sole domain where regulatory efforts focused until then. Rather, they applied, albeit to a certain extent, also to non-international armed conflicts, that is, situation of ‘protracted armed violence between organized armed groups and a State, or between such groups within a State.’[[56]](#footnote-56) As such, Common Article 3 of the Conventions detailed the minimum provisions that parties to the conflict were bound to respect in the course of a non-international armed conflict. These consisted in the obligation to give medical assistance to the wounded and sick, as well as in a general obligation to treat with humanity ‘persons taking no active part in hostilities’, including ‘members of the armed forces who have been placed *hors de combat* by reason of sickness, wounds, detention, or any other cause’. In order to give full effect to the obligation, CA 3 set out a series of prohibition that applied ‘at any time and any place whatsoever’ and included the following acts:

‘’ (a) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

 (b) Taking of hostages;

 (c) Outrages upon personal dignity, in particular degrading and humiliating treatment;

 (d)the passing carrying of sentences and the out of execution without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized people. ‘’[[57]](#footnote-57)

While the Geneva Conventions represented the first step of the process of humanization, their two Additional Protocols further enhanced the degree of protection afforded to the civilian population, by detailing the so-called ‘law of targeting’, a term of art employed to describe a set of rules designed to restrict the amount of violence that belligerents could lawfully deploy in the battlefield. Thus, the Protocols codified the structural-organizational principle of distinction between civilians and combatants, which is now regarded as one of the quintessential principles of the *jus in bello*, and according to which combatants cannot, under any circumstance, intentionally attack civilian and civilian objects, but shall instead target only military objectives.[[58]](#footnote-58) This basic rule is then broken down in more detailed provisions that prohibit certain means and methods of warfare, such as starvation, or intentionally attacking objects indispensable for the survival of the civilian population, like food deposits or water supplies.

Furthermore, the Additional Protocols introduced the principles of proportionality and precaution, both of which can be seen as logical corollaries to the former. Thus, the principle of proportionality prohibits combatants to launch an attack that, while directed against a lawful target, would result in an amount of expected collateral damage (that is, incidental loss of life, injury to civilians, destruction of objects or a combination thereof) which would be excessive in comparison to the military advantage anticipated from the attack.[[59]](#footnote-59) With regards to the rules on precaution, they require belligerents to take a series of measures that encompass both the planning, preparation and launching of an attack, including the obligation to take all ‘feasible’ precautions in order to avoid or minimize collateral damage, as well the obligation to cancel or suspend an attack if it becomes apparent that it would violate the principles of distinction and proportionality.[[60]](#footnote-60) Furthermore, additional measures are incumbent on the defending party, requiring them to segregate lawful military targets from civilian objects, and endeavour to remove the civilian population form the vicinity of military objectives, in order to protect the civilian population from ‘the dangers arising from military operations.’[[61]](#footnote-61)

In addition to the Geneva Conventions and their Additional Protocols, there has been a *stratum* of codification that filled normative gaps in other areas. As such, regulatory efforts focused, to name a few, on increasing the protection of certain selected categories of individuals (such as children) and objects (hospitals, places of worship, even ‘broader’ categories like the natural environment) and in prohibiting the employment of specific weaponry (such as nuclear, chemical and bacteriological weapons, blinding lasers, and anti-personnel landmines). Finally, it is worth mentioning that, while not related to the creation of new rules of IHL *per se*, the humanization process has inspired the development of that branch of international law known as International Criminal Law (‘ICL’ thereinafter). In this regard, ICL aims at improving the effectiveness and compliance with IHL by creating a regime of international criminal responsibility for individuals who have been found guilty of perpetrating serious violations of international humanitarian law. Thus, aside from the experience of the post-WWI International Military Tribunals (‘IMTs’) at Nuremberg and Tokyo, the birth of ICL can be traced back with the establishment of the International Criminal Tribunal for the Former Yugoslavia (ICTY) by United Nations Security Council Resolution 827/1993,[[62]](#footnote-62) followed by the institution of the International Criminal Tribunal for Rwanda under UNSC Resolution 955/1994.[[63]](#footnote-63) Both Tribunals implemented a model of jurisdiction based on the prosecution of selected categories of international crimes, that is: grave breaches of the Geneva Conventions, violations of the laws and customs of war, crimes against humanity, and genocide. This model has been implemented, almost identically, in the Statute of the International Criminal Court, adopted in Rome in 1998.

In conclusion, the emergence of a principle of humanity continues, to this day, to influence the norm-creation process of IHL and extend its protective scope, thus contributing to the humanization of International Humanitarian Law.

### 2.2. Humanization of IHL and rule interpretation.

The second aspect in which the process of humanization impacts IHL is in the ambit of interpretation, where there has been a willingness, especially prevalent among international courts and the academic community, to adopt a humanity-driven approach to existing norm of IHL. In this regard, one of the most impactful examples of how this process works in practice can be found in the *Tadic* case before the Appeals Chamber of the ICTY. The defendant, Dusko Tadic, had been charged with the commission of grave breaches of the Geneva Convention (Art. 2 ICTY Statute), crimes and against humanity (Art. 5 ICTY Statute) and violations of the law and customs of war (Art. 3 ICTY Statute). In its appeal, the defendant argued that the Court lacked subject-matter jurisdiction over the alleged crimes, since the competence of the Court could be exercised only with regards to crimes committed in the context of an international armed conflict. Therefore, the Court could not prosecute crimes acts which, even if they were proven, were nonetheless perpetrated in the context of a non-international armed conflict, such as that took place in the former-FRY. The Court rejected the grounds of appeal of Mr. Tadic in its entirety, arguing instead that the conflict in the former Yugoslavia qualified as international in character. More importantly, the Court noted that, even in the hypothesis in which the conflict could be considered as internal, Art. 3 of the Statute would still be applicable, making the defendant subject to prosecution for having committed war crimes. In framing its argument, the Court begun with a textual interpretation of Art. 3 ICTY Statute, noting that its wording did not specify (as opposed to Art.2) whether the crimes needed to be committed in an international armed conflict, so it was theoretically possible that the scope of what constituted ‘violations of the laws and customs of war’ could extend to internal armed conflict. Then, the Appeals Chamber moved on to determining the existence of customary international humanitarian rules applicable to international armed conflict. In this regard, the Court found rules pertaining to the protections of civilians, certain categories of objects (such as cultural property) and a ban on different means and methods of warfare, such as on the use of chemical weapons and perfidy. What is more interesting is the reasoning employed to reach such a conclusion. After having pointed out how the dichotomy between interstate wars and civil war had been rendered obsolete by the emergence of a human-right based approach, the Trial Chambers declared that:

“Elementary considerations of humanity and common sense make it preposterous that the use by States of weapons prohibited in armed conflicts between themselves be allowed when States try to put down rebellion by their own nationals on their own territory. What is inhumane, and consequently proscribed, in international wars, cannot be but inhumane and inadmissible in civil strife.’[[64]](#footnote-64)

The above passage shows us how humanity-based considerations have been anchored to the legal reasoning and used as a mean of extending the scope of application of the *jus in bello* in areas previously unregulated areas. In the *Tadic* case, this was reflected in the application by analogy of the rules pertaining to International Armed Conflicts to Non-International Armed Conflicts. But examples of this tendency are abundant in the jurisprudence and have led, *inter alia*, to the widening of the meaning of ‘protected persons’ under the Geneva Conventions, enhanced the scope of application of the right to repatriation of Prisoners of War, contributed to the lowering of the threshold for the prosecution of crimes against humanity, which no longer need to be causally connected with a situation of armed conflict (whether internal or international in character). Furthermore, these efforts are not peculiar to the international jurisprudence, but they extend within the academic community and non-governmental organization, the most impactful attempts at humanizing warfare being made by the International Committee of the Red Cross, which has proposed a revision of the principles governing the use of force against combatants in its 2009 ‘Interpretive Guidance to the Notion of Direct Participation in Hostilities’.[[65]](#footnote-65)

## 3. Objective and structure of the thesis.

Despite speaking of a ‘humanization’ of warfare might seem contradictory, the impact of the principle of humanity on the norm-creation and rule interpretation of the *jus in bello* has had an undeniable, net-positive effect on the conduct of hostilities. Albeit imperfect in terms of application and enforcement, rules such as those prohibiting the employment of certain means and methods of warfare or the targeting of civilian have directly contributed to the reduction of the adverse effects of warfare, as it is now recognized that the number of casualties resulting from armed conflicts worldwide is declining since 1946.

Considering this, the purpose of my research is to discuss how we can ‘humanize’ the conduct of hostilities in cyberspace by employing a human dignity-based interpretation to the rules of targeting. In order to do so, the main task of Chapter 1 will be that of demonstrating how the humanization of IHL is the result of the polarizing dynamic between the principles of military necessity and humanity. In order to demonstrate why the two principles stand in stark opposition between each other, I will analyse the constitutive elements of both, claiming the military necessity operates as a permissive principles, but its scope of application has been progressively limited by the principle of humanity, which is founded on the respect of the idea of human dignity. Consequently, a significant part of the Chapter will be devoted to explaining the meaning of the concept of human dignity, its evolution and its foundational role within IHL. The Chapter, after having highlighted how the principles of military necessity and human dignity interact with each other in the rules of targeting, will then pose the following question: can we apply a human dignity-oriented reading to the rules of cyber-targeting in order to further promote the humanization of IHL? The question will be tackled by the following chapters, beginning with Chapter 2, which will clarify what kind of cyber-operation amounts to an ‘attack’ for the purposes of IHL, arguing that cyber-attacks are different from conventional attacks because they are able to endanger the dignity of the civilian population in unprecedented ways. This calls for a qualitative re-thinking of the concept of violence which lies at the heart of the notion of attack. The resulting definition of cyber-attack will be of crucial importance for the application of the rules on targeting pertaining to the principles of distinction, proportionality and precaution. Therefore, Chapter 3 will discuss the application to cyber of the principle on distinction between civilians and combatants, analysing firstly the notion of combatancy in its different components before moving on to examine the notion of ‘direct participation in hostilities’ (DPH). Then, Chapter 4 will tackle the distinction between civilian objects and military objectives, by breaking down the requirements of ‘effective contribution to military action’ and ‘definite military advantage’, focusing on how they influence the dynamic between military necessity and the principle of humanity, as far as cyberwarfare is concerned. In this regard, it will be argued that, since the scope of who and what can be targeted in the cyber domain is expanded, this puts the civilian population at an increased risk. Therefore, the task of limiting the potential adverse consequences of cyber-attacks must be taken on by the principles of proportionality and precaution. Chapter 5, then, explores the application of the principle of proportionality in the cyber domain, discussing the notions of ‘incidental damage’ and ‘anticipated military advantage’, and emphasizing how the protection of the civilian population and their dignity would greatly benefit from the inclusion, within the proportionality analysis, of so-called ‘reverberating effects’ of cyber-attacks. Finally, Chapter 6 deals with the rules on precautions in attacks and against the effects of attacks, explaining how they are influenced by cyber-warfare and how this affects the dualism between military necessity and the principle of humanity.

## 4. Methodology and originality.

The methodology I will intend to use will be entirely library based. It will consist, primarily, in a combination of historical and doctrinal methods. As such, I will firstly discuss the origins and the evolution of the concepts of human dignity, military necessity and of the fundamental principles of the law of armed conflict. Secondly, these concepts and principles will be contextualized within my theoretical framework by using the relevant jurisprudence of international, regional and national courts and tribunals, the views of legal scholars as well as State practice.

With regards to how the subject of cyber has been discusses in the literature, the two leading monographs, *Cyber warfare and the Laws of War* by Heather Harrison Dinniss,[[66]](#footnote-66) and *Cyber Operations and the Use of Force* in International Law by Marco Roscini,[[67]](#footnote-67) examine whether or not IHL is applicable to cyber warfare in the first place, and discuss the application to cyber of specific principles and rules of IHL. Selected publications from legal journals show that different academic have written on specific issues about the relationship between the law of targeting and cyber-warfare, such as the principles of distinction[[68]](#footnote-68), proportionality, precautions in attack[[69]](#footnote-69) and the concept of Direct Participation in Hostilities.[[70]](#footnote-70) In this regard, the underlying assumption of the vast majority of these articles is that the law of targeting applies only to cyber-attacks which cause physical violence, an interpretation which is radically different from my approach. Significantly, debates in the academic literature have focused on whether or not *digital data* are ‘objects’ under IHL[[71]](#footnote-71), with scholars divided on the matter. While these articles share a similarity with part of the subject-matter of my research, their treatment of the topic did not mention any implication for the ‘humanization of IHL’. By contrast, the originality of my project relies, firstly, on employing a concept of human dignity to explain how the process of humanization of IHL is reflected in the rules of targeting and, secondly, on applying this human dignity-oriented framework to the cyber scenario. As such, my aim is to determine whether this interpretation can ‘humanize’ the conduct of hostilities in cyberspace, and therefore positively contribute to the protection of the civilian population from the adverse effects of cyber-attacks. Having defined the objective of the thesis, it is submitted that the topic of attribution of cyber-attacks remains largely outside the scope of my research. As such, I will not be discussing any technical challenges that may arise when tracing back a cyberattack to its perpetrators. As such, whenever I will be referring to a cyberattack during the course of my thesis, either real or fictitious, it will be assumed that said cyberattack has been successfully attributed to its source from a technical point of view.

Similarly, this thesis will not discuss the legal issues related to attribution with regards to international law generally, such as establishing the responsibility of a State for an internationally wrongful act, or what is the standard of proof that should be considered in the cyber context.[[72]](#footnote-72) Having said that, I will nonetheless mention some legal aspects of attribution related to IHL, specifically in Chapter 4, when discussing how the status of Prisoner of War (POW) applies to the cyber context.[[73]](#footnote-73)

# Chapter 1. The relationship between the principle of military necessity and human dignity-based considerations within the law of targeting. Cyberwarfare’s interpretive challenges.

The modern law of armed conflict, also known as International Humanitarian Law (‘IHL’), is the result of the balance of two, opposing, normative principles, those of military necessity and humanity. While the former allows belligerents to use violence to accomplish their military goals in order to prevail over the enemy, the latter serves the purpose of limiting the suffering caused by armed conflict to the civilian population and, albeit to a lesser extent, to combatants, by protecting their human dignity. Considering this, the objectives of the Chapter is twofold; first of all, it aims to contextualize the meaning, the function and the scope of application of the two principles, as they represent the two driving forces that shape the normative content of IHL; secondly, the Chapter aims to highlight the interpretive challenges inherent in the humanity-necessity balance within the *jus in bello*, and what is the impact of cyberwarfare on their relationship. To do so, Section I of the Chapter discusses the principle of military necessity, comparing it with different forms of ‘necessity’ in international law, namely under the international human rights law regime and under the law on the use of force, to claim the function of the principle, within the law of armed conflict, is predominantly permissive, rather than restrictive. Section II argues that the permissive function of military necessity is counterbalanced, at the normative level, by the principle of humanity, which is founded on respect for human dignity: in this regard, the origins and the evolution of the concept will be explored. Section III illustrates how the principles of military necessity and humanity relate to each other in the *jus in bello*, arguing that they are especially interwoven in the principles on distinction, proportionality, precaution and unnecessary suffering, a set of provisions forming the so-called ‘law of targeting’. Section IV concludes by setting the stage for the argument that will be developed in the following chapters: namely, to what extent it is possible to apply a human-dignity oriented reading of the rules of targeting to the emerging phenomenon of cyberwarfare, and whether it will result in a beneficial or detrimental effect upon the conduct of hostilities.

## 1. The principle of Military Necessity and its functions in the *jus in bello*.

The earliest formulation of the concept of military necessity appears in the Instructions for the Government of Armies in the Field, General Order n. 100, better known as the ‘Lieber Code’, from the legal scholar tasked by United States President Abraham Lincoln to issue regulations on the conduct of hostilities during the American Civil War.[[74]](#footnote-74) Thus, Art. 14 of the Lieber Code defines the concept in the following terms:

‘Military necessity, as understood by modern civilizations, consists in the *necessity* of those measures which are *indispensable* for securing the end of the war, and which are lawful according to the modern law and usages of war.’[[75]](#footnote-75)

The crucial point of the definition lies in the word ‘necessity’. To properly understand its meaning within the *jus in bello*, I will discuss its or origins and what functions it performs in international law. Historically, the principle of necessity has been closely connected to the right of self-preservation of States.[[76]](#footnote-76) In this regard, the latter concept was regarded, in the early days of international law, as a ‘fundamental right to existence’ of the State, encompassing its physical, human and moral preservation.[[77]](#footnote-77) Its function was that of a ‘justification for the priority between two subjective rights’,[[78]](#footnote-78) allowing the invoking State to take measures inconsistent with the dictates of positive international legal norms and to violate the rights of other States whenever it felt that its security was threatened.[[79]](#footnote-79) In this context, the principle of necessity was a component of the right of self-preservation, since it ‘described the conditions that needed to be in place to justify the forceful protection by a State of its legitimate interests.’[[80]](#footnote-80) The doctrine of necessity as a component of the right of self-preservation was thus employed in a wide array of circumstances, such as in the case of recourse to force by a State against another State, or to justify departures from the rules regulating the conduct of hostilities, which restricted the amount of force that a State could lawfully employ during wartime.[[81]](#footnote-81) Eventually, the doctrine of self-preservation was progressively abandoned, as it was perceived to be dangerous for the existence of the international legal order.[[82]](#footnote-82) Yet, today the concept of necessity still retains its relevance in contemporary international law, where it operates as a justification,[[83]](#footnote-83) thus allowing, under exceptional circumstances, the non-performance of a certain obligation by a State or by an individual.[[84]](#footnote-84) Intended as such, the principle appears in several areas of international law. Within the law of State Responsibility, it is considered a circumstance precluding the wrongfulness of an otherwise internationally unlawful act; under the law on the use of force, it is one of the conditions for the exercise of the law of self-defence; within the International Human Rights Law regime, necessity, and the lack thereof, determines whether the violation of one’s right can be considered justified. The concept of necessity plays a similar role in the law of armed conflict, where it is considered as an exception specifically accounted for by certain rules. Note, however, that there are differences between these instances of ‘necessity’ and the principle of military necessity under the law of armed conflict. More specifically, the above-mentioned applications of the principle of necessity can be characterized as restrictive, given that they are subjected to and limited by the existence of certain stringent conditions, whereas the notion of military necessity, while maintaining its status as a justification, is instead an essentially permissive principle.[[85]](#footnote-85) Accordingly, the following section will contextualize the differences between the two conceptions, by describing how restrictive models of the principle of necessity are applied in International Human Rights Law regime as well as in the law of the use of force and contrasting them with the application of the principle of military necessity in IHL.

### 1.1 Restrictive models of necessity: the use of lethal force under International Human Rights Law.

International Human Rights Law is a branch of international law that aims to guarantee the rights of those individuals under the jurisdiction of the State, usually in times of peace. Accordingly, and especially with regards to the use of lethal force, any action of the State that infringes upon an individual’s right to life must be exceptional, and subject to a so-called ‘law enforcement model’, which is built on three different assumptions. Firstly, every individual shall benefit from the presumption of innocence; secondly, persons suspected of planning or perpetrating serious criminal acts should be arrested, detained and interrogated with due process of law; thirdly and finally, is there is credible evidence that they committed a crime, they should be afforded a fair trial. In practice, this means that under IHRL law the principle of necessity has been applied very restrictively under different sub-regimes of IHRL. In the following, I will briefly discuss the interpretation given to it by the Human Rights Committee (HRC) and the European Court of Human Rights (ECtHR) under, respectively, Art.6 of the ICCPR and Art. 2 of the ECHR.

#### 1.1. i. Necessity under Article 6 ICCPR.

According to Article 6 of the ICCPR, ‘no one shall be *arbitrarily* deprived of his life’[[86]](#footnote-86). The notion of necessity is the deciding factor in the determination of what constitutes an arbitrary deprivation of life. In this regard, the Human Rights Committee has made clear that two different elements must concur.

Firstly, there must be an imminent threat of death and serious injury on the part who is using lethal force.[[87]](#footnote-87) The assessment of what constitutes an imminent threat may be determined, on a case-by-case approach, by actions on the part of the state agents, such as the use of an unheeded warning or resort to non-lethal means which prove to be ineffective.[[88]](#footnote-88) Secondly, there must be an absence or lack of any viable alternative to the use of lethal force. In other words, either the alternatives to the use of lethal force have been employed to no avail or, given the exigencies of the situation, there are no alternative to the use of lethal force and its use is necessary to prevent death or serious injury.[[89]](#footnote-89) An example of the application of these criteria is exemplified the case of *Maria Suarez de Guerrero v Colombia*, where Colombian police launched an operation for rescuing the Ambassador of Colombia to France, who had been kidnapped by a guerrilla organization some days earlier. During the raid in the house where the Ambassador was believed to be held captive, Colombian police shot and killed several of the alleged kidnappers, including Mrs. De Guerrero. During the proceedings, it was found out that neither the Ambassador, nor the alleged suspects were present at the house during the raid, further being revealed that the police waited the arrival of alleged suspects at the house in order to arrest them. Contrary to the police allegations that the killing of the suspects was the result of their attempt to resist a lawful arrest by ‘brandishing and firing various weapons’,[[90]](#footnote-90) it was revealed that the victims were unarmed, and several of them shot at point blank. Accordingly, the HRC determined that the action taken by the Colombian Police was in violation to Art. 6 ICCRP, as Mrs. Guerrero and the other suspects did not pose an imminent threat at that given moment and, furthermore, they were not given any warning, or opportunity to surrender.[[91]](#footnote-91)

#### 1.1. ii. Necessity under Art. 2 ECHR.

Such an approach to necessity in the context of the right to life is particularly stringent and plays a similarly important role in relation to Art. 2 ECHR. In this regard, it must be premised that within he ECHR framework the principle of necessity is one of the components a proportionality analysis (PA) that takes place in human rights adjudications ‘whenever a government has infringed upon an individual’s liberty, but believes it has reason to do so’.[[92]](#footnote-92) The PA has four prongs. The first prong determines if the governmental aim is legitimate or not; in the latter case, the government action is unlawful, and no further analysis is needed. If the government is, in fact, pursuing a legitimate aim, the second state of the proportionality test demands that the means used by the government to attain its legitimate aims were suitable; thirdly, the government action must be ‘necessary’ to achieve such legitimate aim; finally, the government action must be proportionate.[[93]](#footnote-93)

Secondly, unlike Art. 6 ICCPR, Art.2 ECHR is very clear in requiring that deprivation of life in pursuit of a legitimate aim must result from a use of force which is ‘*no more than absolutely necessary*’,[[94]](#footnote-94) a wording that has been recognized by the ECtHR in the *Handyside* case as synonymous with *indispensable*.[[95]](#footnote-95) In practice, a determination of when the use of lethal force is absolutely necessary involves a methodological distinction of the principle of necessity, as applied in the PA, between its qualitative, quantitative and temporal elements, as noted by Nils Melzer.[[96]](#footnote-96) As such, the qualitative element looks at whether the legitimate aim of the operation pursued by State agents can be achieved by means not involving the use of potentially lethal force, as explained in cases such as *McCann v. United Kingdom.* The facts revolved around an operation launched by UK and Spanish police aimed at stopping a terrorist bombing that members of Provisional Irish Republican Army (IRA) were allegedly planning in Gibraltar. Believing that the suspects had a bomb, the military handled the operation, shooting and killing three of the suspects, although it was later revealed that they were unarmed. The Court, despite accepting the soldiers’ view that they believed the suspects to be armed, found the operation in violation of Art. 2 ECHR, arguing that the soldiers’ action were the result of lack of proper instruction and care on part of the authorities, pointing out, in particular, the fact that the authorities did not attempt the suspects at the Gibraltar border, and for not considering whether the information as to the suspects having a remote control detonation device could have been incorrect.[[97]](#footnote-97)

The quantitative element of necessity demands, instead, that no more than the minimum amount of necessary force has to be used in the given situation or, in other words, ‘whether or not the degree to which potential lethal force is employed is more hazardous to human life than absolutely necessary to achieve a legitimate aim.’[[98]](#footnote-98) This is shown in *Gulec*, a case revolving around a violent demonstration in Turkey, in which some 3,000 people participated, and which was quelled by the Turkish police with the use of firearms, resulting, eventually, in the death of fifteen-year-old Ahmet Gulec. The Court, stating the need to find a balance ‘between the aim of the operation and the means employed to obtain it’, criticized the fact that the Turkish authorities were ill-equipped to handle a violent demonstration, as they had not been provided with ‘truncheons, riot shields, water cannon, rubber bullet or tear gas.’[[99]](#footnote-99) Hence, the Court found that the use of *potentially lethal force* by the Turkish authorities was in contravention of Art. 2(2) ECHR, as it was not within the meaning of absolute necessity. Finally, the principle of necessity has a temporal dimension, whereby a violation of Art. 2 ECHR exists when lethal force, in the given moment in which it was used, was not or no longer absolutely necessary to achieve e legitimate aim. An application of this element of the necessity principle can be seen in *Nachova*,[[100]](#footnote-100) where a military Major shot and killed, during an arrest attempt, two Bulgarian citizens of Roma origin who absconded from a military construction site where they were held in custody. In this case, the Court found, *inter alia*, a violation of Art. 2 since there was no imminent threat posed by the two victims at the moment when lethal force was employed, which was rather motivated on grounds of racial discrimination.[[101]](#footnote-101)

From the above analysis, it can be concluded that the principle of necessity operates as a restrictive principle under IHRL, especially when it is applied to the use of potentially lethal force. In this regard, and despite some interpretative distinctions, it is nonetheless possible to trace some commonalities between the ICCPR and the ECHR; that is, the principle of necessity requires that any use of potentially lethal force must submit to a least-harmful means approach. As it will be shown *infra*, these elements of necessity can also be observed under the *jus ad bellum*.

### 1.2. Restrictive models of necessity: the law on the use of force.

The law on the use of force is that branch of international law that regulates recourse to armed violence by States in their international relations. Its foundational norm is Art 2(4) of the United Nations Charter, according to which ‘[all] States shall refrain in their international relations from the threat or use of force against the territorial integrity and the political independence of every other State, and in any other manner inconsistent with the purposes of the United Nations.’[[102]](#footnote-102) The prohibition, which possesses customary status,[[103]](#footnote-103) and is considered a *jus cogens* norm,[[104]](#footnote-104) is complemented by two exceptions, namely collective action undertaken by the Security Council, acting under Chapter VII, and self- defence under Art. 51 of the Charter: according to the latter, ‘nothing in the present charter shall impair the *inherent* right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations [..]’.[[105]](#footnote-105)

Within the law of *ad bellum* self-defence, the concept of necessity delimits the instances in which a State is lawfully entitled to use force against another State. Restriction on the use of force by States pre-date modern international law and can be traced back to the Just War Theory (JWT) doctrine. The JWT sought to distinguish just from unjust wars, and the concept of necessity was one of the requirements under which recourse to force could be morally justified. In this regard, the most important interpreter of the JWT tradition is Hugo Grotius, who argued that necessity was limited only to circumstances of immediate and imminent danger of being attacked,[[106]](#footnote-106) and recourse to force was morally justified only when there was no other less harmful mean to avoid the danger.[[107]](#footnote-107) The Grotian perspective, argues Ohlin, recognizes that there is a right of State to defend themselves using force, but this right is ‘severely limited by certain temporal and spatial considerations that are embodied in a last resort or *ad bellum* necessity condition.’[[108]](#footnote-108)Such an approach of necessity has retained its theoretical influence even after the JWT doctrine progressively lost traction after the peace of Westphalia, as evidenced, *inter alia*, by the terminology employed in the most illustrious antecedent of the contemporary notion of self-defence, the *Caroline* case. Often referred to as the *locus classicus* of self-defence,[[109]](#footnote-109) the Caroline case revolved around the destruction, by British troops, of a US-owned steamboat that took place between the United States and the British-Canadian border in 1837. In the following correspondence between the American Secretary of State and the British Special Plenipotentiary, the former remarked how the British action could be legally justified, but under the condition that it had been required by a ‘necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation.’[[110]](#footnote-110) Furthermore, the measures taken in self-defence should not be ‘unreasonable of excessive; since the act justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it.’[[111]](#footnote-111) This formulation of self-defence resembles Grotius’ idea of necessity, as it focuses on the imminence of danger and the lack of least-harmful means as necessary conditions for the recourse to force. As we shall see, the modern conception of *ad bellum* necessity possesses similar features.

#### 1.2. i. Necessity under the jus ad bellum: the notion of ‘armed attack’ in its material and temporal elements.

The first element of the necessity requirement in the modern *jus ad bellum* relates to the fact that an armed attack must occur before a State can exercise its right to self-defence. For the purposes of the present argument, two elements of the notion of armed attack must be considered. Firstly, the objective element of Art.51 relates to what kind of acts may qualify as an armed attack. In this regard, the ICJ, while not expressly defining the *rationae materiae* of the concept of armed attack, has interpreted it as a higher threshold requirement compared to the notion of ‘use of force’ under Art. 2(4) of the UN Charter. In the *Nicaragua* case, the Court argued that there is necessary ‘to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.’[[112]](#footnote-112) What differentiates the former from the latter, in the opinion of the Court, is merely a matter of *scale and effects*.[[113]](#footnote-113) The distinction between the two notions has been subsequently confirmed in the *Oil Platforms* judgments, where the ICJ made also clear that an armed attack may also occur when a series of acts, each of them constituting a mere use of force, can, if taken cumulatively, reach the threshold of armed attack.[[114]](#footnote-114) Despite doctrinal criticism, the existence of a *de minimis* threshold under which no force in self-defence can be invoked has been subsequently confirmed in the *Oil Platform* judgment; moreover, it can also be inferred from the *travaux preparatoires* of the UN Charter,[[115]](#footnote-115) and is now accepted as a matter of State practice.

The second aspect of the notion of armed attack relates to its temporal dimension. In this regard, the wording of Art. 51 is clear on specifying that the right to use force in self-defence arises ‘if an armed attack *occurs*’, thus suggesting that a State may use force not only after an armed attack has occurred, but also in response to an armed attack that *about to happen*. While is intuitive to argue that a State should not wait to be hit by an armed attack to lawfully exercise its right of self-defence under the UN Charter, the *crux* of the matter relates on how *imminent* an armed attack has to be before the State can act. In this regard, imminence must be interpreted narrowly, so that recourse to armed force by a State can only be allowed in response to an armed attack that is already underway, in what Yoram Dinstein has termed as *interceptive* self-defence.[[116]](#footnote-116) The focal point of this interpretation is too look at who embarked upon an apparently irreversible course of action in order to determine when an armed attack has begun, instead of determining who has fired the first shot.[[117]](#footnote-117) As a matter of law, the doctrine of anticipatory self-defence in unquestionably lawful and generally accepted as a matter of State Practice.[[118]](#footnote-118)

In conclusion, when it comes to the notion of armed attack as a sub-component of necessity in the *jus ad bellum*, the requirement has been interpreted narrowly, as it requires the existence of a use of force of ‘the most grave forms’, which must have already happened or be underway.

#### 1.2. ii. Necessity under the jus ad bellum: the component of ‘last resort’*.*

The second element of the necessity criterion requires the state who has been the victim of an armed attack to have exhausted all other, alternative peaceful means before resorting to force in self-defence. In this regard, Ago notes that the action taken in self-defence must be necessary in the sense that the State victim of an armed attack ‘must not […] have had any means of halting the attack other than recourse to armed force. In other words, had it been able to achieve the same result by measures not involving the use of armed force, it would have no justification for adopting conduct which contravened the general prohibition against the use of armed force.’[[119]](#footnote-119) The last resort requirement of necessity enjoys unanimous support in present day legal doctrine, and its application is uncontroversial, despite being, as long as self-defence in response to a prior armed attack is concerned, of ‘relative practical significance’.[[120]](#footnote-120) In fact, as noted by Tom Ruys, ‘practice indeed indicates that the need to exhaust peaceful means only plays a subsidiary role for the assessment of self-defence claims in response to a prior attack, and that unlawfulness will only result when a manifest unwillingness to address diplomatic channels can be demonstrated.’[[121]](#footnote-121)

#### 1.2.iii. Necessity under the jus ad bellum: the component of ‘immediacy’.

The final component of *ad bellum* necessity demands that there must be some temporal proximity between the armed attack suffered by the victim State and its use of force in self-defence. The *rationale* behind the immediacy requirement is to distinguish between lawful actions of self-defence and armed reprisals, which are unlawful under international law. In this regard, State practice and doctrine have interpreted immediacy with a certain degree of flexibility, by accounting for various factors that can influence the time-frame after which acting in self-defence in response to an armed attack would be considered permissible. These include, among others, the exhaustion of alternative, peaceful means to settle the controversy; the gathering of intelligence and information in order to act in self-defence; the geographical distance between the victim State and the aggressor State; and, if the State has been the victim to a series of armed attack – rather than an isolated one - the need to use force to remove continuing threats to that State’s security.[[122]](#footnote-122)

### 1.3. The principle of military necessity and its functions.

The previous paragraphs have highlighted how the notion of necessity operates as a restrictive principle with regards to the use of force in the *jus ad bellum* and International Human Rights Law. Does the principle of necessity operate any differently within the *jus in bello?* The first analytical step to answer the question takes us back to the basic definition of Art. 14 of the Lieber Code, according to which:

‘Military necessity, as understood by modern civilizations, consists in the *necessity* of those measures which are *indispensable* for securing the end of the war, and which are lawful according to the modern law and usages of war.’[[123]](#footnote-123)

The International Military Tribunal at Nuremberg, in the *Hostage* case, described the concept in a similar vein:

‘Military necessity permits a belligerent, subject to the laws of war, to apply any amount and kind of force to compel the complete submission of the enemy with the least possible expenditure of time, life, and money.’[[124]](#footnote-124)

The definition of the concept, with a choice of words that combines elements from Art. 14 of the Lieber code as well as from the *Hostage* case, is now adopted by most military manuals.[[125]](#footnote-125)

From the above definitions one can infer two different elements. First, military necessity permits certain measures which must be connected with the legitimate aim of armed conflict, that is, the submission of the enemy. In practice, the nature of those measure has been specified already by Art. 15 of the Lieber Code, which included ‘all direct destruction or limb of armed enemies, and of other persons whose destruction is incidentally unavoidable in the armed contest of the war; […] the capturing of every armed enemy, and every enemy of the importance to the hostile government; [..] all destruction of property, and obstruction of the ways and channels of traffic, travel, or communication, and of all withholding of sustenance or means of life from the enemy’ among others.[[126]](#footnote-126) Ever since, it can be argued that the scope of what is allowed by military necessity remained relatively untouched by the subsequent strands of codification of the *jus in bello*. To put it differently, the current state of IHL allows to kill combatants and to destroy military objectives in pursuit of the goal of the armed conflict; furthermore, it does not prohibit the killing of civilians when it is ‘incidentally unavoidable’, that is, when they are considered lawful collateral damage in accordance with the proportionality principle under IHL. Secondly, these measures must be in accordance with the laws of war, as we can see under Art. 16 of the Liber Code, which prohibits acts such as the infliction of cruelty, torture, the use of poison or wanton devastation. [[127]](#footnote-127)

The need to place legal limits to the application of the principle of military necessity was motivated by the emergence, during the late nineteenth century, of the doctrine of *Kriegsrason*. Of German origin, the maxim ‘*kriegsraison geht vor kriegsmanier*’ can be aptly translated as ‘the necessities of war shall prevail over the laws of war.’ In this sense, necessity was intended as a principle outside the law that could be invoked whenever military commanders saw it fit in order to accomplish their goals, placing military interests beyond all regulation.[[128]](#footnote-128) As such, it has been argued that the *Kriegsrason* doctrine was nothing more than a re-statement of the principle of self-preservation to the domain of warfare.[[129]](#footnote-129) But the application of this version of military necessity has been resisted since the earliest stages of the law of armed conflict; already the St. Petersburg Declaration of 1868, in banning the use of projectiles under 400 grams of weight, recognized that ‘the right of belligerents to injure the enemy is not unlimited.’[[130]](#footnote-130) Most importantly, the validity of the *Kriegsrason* was unequivocally rejected in the *Hostage* case, where the defendants argued that prohibition on intentionally killing civilians could be overridden by considerations of military necessity. The Court disagreed, noting that ‘international [humanitarian] law is prohibitive law’ and as such ‘does not permit the killing of innocent inhabitants for purposes of revenge or the satisfaction of a lust to kill […]’; on the contrary, any destruction, to be justified ‘must be imperatively demanded by the necessities of war’.[[131]](#footnote-131)

The above considerations bring us to an in inquiry as to the meaning of ‘necessity’ under the *jus in bello*, where the academic doctrine is divided as to whether the concept performs a restrictive function, a permissive function, or both. In the following paragraph I will argue that military necessity is predominantly a permissive principle of IHL and performs a restrictive function only when it is considered as an exception in specific IHL provisions.

1.3.i. Military Necessity as a permissive principle.

The argument that identifies military necessity as a permissive principle stems from a comparison of how the very meaning of the word ‘necessity’ in IHL diverges from its *jus ad bellum* and IHRL counterparts. As it has been discussed in the previous section, a restrictive model of necessity requires the existence of a situation of imminent threat, which legitimizes the use of lethal force in the first place, and a least-harmful approach whereby lethal force can be lawfully employed only when other, non-lethal means have been exhausted or, given the situation at hand, are deemed to be ineffective: these two elements are present both in the law in the use of force and in IHRL. However, *Jus in bello* necessity lacks these requirements, as the use of lethal force is conditional only upon the pursuit of the legitimate aim of the armed conflict which is, as noted earlier, the submission of the enemy. For the accomplishment of this objective, belligerents are licensed to kill combatants and to use any amount of force they deem necessary in the circumstances of the case. Once an individual qualifies as a combatant, he may be attacked ‘at all times and in all circumstances’,[[132]](#footnote-132) regardless of whether he represents an imminent threat and whether less than lethal amounts of force could be used against him; rather, prohibitions on the use of force are imposed on belligerents only when a combatant is put *hors de combat* and only if the means and methods of warfare used are of a nature to cause superfluous injury or unnecessary suffering. This represents the essential element of the permissive nature of military necessity under IHL, and stems from the assumption that a combatant, by virtue of their status, will constitute an imminent threat which can be contrasted with no other means but the use of lethal force; given that such a presumption is absolute, a Party to the conflict does not need to prove imminence, nor the adoption of a least-harmful means approach.[[133]](#footnote-133)Therefore, it can be argued that, as opposed to its *jus ad bellum* and IHRL counterparts, the concept of *jus in bello* necessity is not synonymous with ‘indispensable’ or ‘leaving no other choice’, but merely as being related to ‘the prompt resolution of the war effort.’[[134]](#footnote-134)Hence, it is submitted that military necessity performs an essentially permissive function.

Against this argument, different authors have adopted the view that military necessity also performs a *restrictive* function. Thus, Niels Melzer has argued that ‘the principle of military necessity prohibits the employment of any kind or degree of force which is not indispensable for the achievement of ‘the ends of the war’, even if such force would not be otherwise prohibited by IHL’.[[135]](#footnote-135) As such, he notes, ‘a direct attack against an otherwise legitimate military target constitutes a violation of IHL if that attack is not required for the submission of the enemy with a minimum expenditure of time, life and physical resources.’[[136]](#footnote-136)This statement raises two counterpoints. The first point raised by Melzer holds that only those measures which are indispensable to prevail over the enemy are allowed, and any kind of degree of force which is not actually necessary for military purposes is prohibited. This claim, which is supported by several scholars,[[137]](#footnote-137) appears, *prima facie*, hardly refutable: after all, the demise of the doctrine of *Kriegsrason* proved that military necessity did not give a license for unrestricted warfare, and that any use of lethal force must be justified by the existence of a military advantage. Acts that bear no actual relation to this goal, such as cruelty or torture, are prohibited, since they are ‘unrelated to the external aim of the war and [are] tethered only to’ a ‘logic of violence for its own sake.’[[138]](#footnote-138) Then, from the same *rationale* should flow the prohibition to intentionally kill civilians or combatants who are placed *hors de combat*, since nothing is gained, in military terms, from using lethal force against them. Yet, one cannot but see how the very ends and aims of warfare can be (and have been) interpreted in various ways, leading to different understandings of what is ‘necessary’ in military terms and, most importantly, to different outcomes when the law is applied to the battlefield. As such, certain approaches to military necessity claim that, for the purpose of overcoming the enemy, it is merely ‘sufficient to disable the greatest number of men’[[139]](#footnote-139), as declared by the Preamble of the St. Petersburg Declaration. Taken to its logical limits, this approach does lead to the conclusion that IHL recognizes that under certain circumstances belligerents are under an obligation to capture, rather than kill, enemy combatants if they do not pose any risk (say, when they are unarmed) to the safety of the attacking forces. That is, most notably, the position endorsed by the ICRC in its *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, which went as far as claiming that ‘it would defy basic notions of humanity to kill an adversary or to refrain from giving him or her the chance to surrender where there manifestly is no need for lethal force to be used.’[[140]](#footnote-140)

On the other hand, views like those epitomized by the doctrine of *Kriegsrason* would yield different results: the very practice of high-altitude indiscriminate bombardment of urban areas, which had been employed by the Allied Powers against Germany during WWII and became infamously known as ‘carpet bombing’, was legitimized by the belief that targeting the civilian population could weaken their morale and consequently shake the consensus on which the Nazi regime was relying on. In other words, targeting the civilian population was perceived, at the time, as being consistent with the goal of prevailing over the enemy. In a similar fashion, when the US-led NATO coalition targeted and destroyed the headquarters of the Radio Television of Serbia (RTS) during the 1999 Kosovo campaign, NATO justified the operation as being part of a ‘campaign to dismantle the FRY propaganda machinery which is a vital part of President Milosevic’s control mechanism.’[[141]](#footnote-141) Certainly, it can be pointed out how such practices represent an unwelcome, yet isolated, resurgence of the *Kriegsrason* doctrine and are in no way indicative of how the principle of military necessity is interpreted today. However, one can go no further than the *Hostage* formulation of military necessity to notice how expansive is the notion of military necessity it endorsed, since every action that can accomplish the aim of warfare and is taken with the ‘least expenditure of life, time and money’ is permitted. In this regard, David Luban has correctly argued that the *Hostage* case ‘remains overwhelmingly slanted in favour of militaries and grants them enormous latitude. Read literally, military necessity includes any lawful act that saves a dollar or a day in pursuit of victory. These are claims of military convenience, not military necessity.’[[142]](#footnote-142) Therefore, a similar interpretation of military necessity would be at odds with the ICRC’s contention that, under certain circumstances, belligerent parties are under the obligation to capture, rather than kill, enemy combatants, because the attempt to capture will most likely result in additional risk of damage for the attacking force. Even assuming that a situation exists in which no life of the attacker would be put in danger by a capture rather than kill approach, it can still be contended that capturing an enemy combatant would probably require a certain expenditure of money and time, if only for granting him the rights associated with Prisoner of War (P.O.W.) status, which would be more expensive as compared to employing lethal force against him. As such, we can see how different approaches as to what is deemed necessary to obtain the submission of the enemy may lead to a permissive, rather than restrictive, conceptualization of the function of military necessity. Therefore, the view according to which military necessity is restrictive simply because it prohibits any conduct which is unrelated to what is necessary to achieve a military end cannot be shared. From the above consideration stems, also, the fact that military necessity, contrary to what is suggested by Melzer, does not impose an obligation to minimize resource expenditure[[143]](#footnote-143). But such an understanding is not supported by law: in fact, ‘excessive, irrelevant or purposeless acts of the belligerent [..] are not *per se* unlawful. Rather, they are unlawful only to the extent that they injure persons, objects and interest protected under international humanitarian law.’[[144]](#footnote-144) On the other hand, any other conduct that does not conform to standards of military efficiency (that is, that does not result in a minimal expenditure of time, life and resources) is permitted under IHL.

#### 1.3. ii. Exceptional Military Necessity as a restrictive form of necessity in International Humanitarian Law*.*

There is, however, one ambit in which military necessity performs a restrictive function, and that is where the *jus in bello* identifies it as an exception. For instance, Art. 23(g) of the 1907 Hague Regulations states that ‘it is especially prohibited to destroy or seize enemy property, unless such destruction or seizure be imperatively demanded by the necessities of war.’[[145]](#footnote-145) Similar provisions can be found, with reference to ‘absolute’, ‘imperative’, ‘exceptional’, ‘unavoidable’ or ‘urgent’ military necessity, both in the four Geneva Conventions and in their two Additional Protocols, providing a various range of derogations, from the right of Protecting Powers to visit the places of interment of prisoners of war,[[146]](#footnote-146) to the prohibition on forcible transfer of protected persons from occupied territory,[[147]](#footnote-147) and even to the prohibition on starvation against the civilian population.[[148]](#footnote-148) In this context, military necessity operates similarly to what necessity does in the Law of State Responsibility, where it is considered as a circumstance precluding wrongfulness, which justifies a conduct contrary to what the law prescribes for ordinary circumstances.[[149]](#footnote-149) The main difference is, however, that no plea of necessity can be invoked *de novo*, but only to the extent it is expressly provided by specific rules;[[150]](#footnote-150) this interpretation has been confirmed by the ILC in its Commentary to the Draft Articles on State Responsibilityand relies on the assumption that if States were allowed to invoke military necessity to justify non-compliance with *any* rule of IHL, this would lead, essentially, to the resurgence of the *Kriegsrason* doctrine, and the whole purpose of the *jus in bello* would be circumvented. In this regard, what makes exceptional military necessity perform a restrictive function are the conditions that need to be present before a party to the conflict can lawfully rely on it: thus, Hayashi has identified the following constitutive elements of exceptional military necessity.[[151]](#footnote-151) Firstly, the measure for which military necessity is invoked was taken for some specific military purpose; secondly, the measure was *required* for the attainment of the military purpose; finally, both the military purpose for which the measure was taken, as well as the measure itself, must be in conformity with IHL. For the purposes of the present argument, the focal point is the second prong of the necessity test, that the measure was *required* for the attainment of a military purpose: this means, *in concreto*, that the measure itself was not only relevant for such a purpose, but, most importantly, it was the least injurious among other relevant measures that were available in a given situation, and the injury it caused was not disproportionate to the gain expected from it. One recent application of the restrictive version of military necessity can be seen in the *Beit Sourik* case before the Supreme Court of Israel,[[152]](#footnote-152) relating to a barrier built by Israel on the border with Palestine, on the Jebel Muktam Hill. In judging the claim made by the representative of Palestinians harmed by the barrier, the court noted that, according to IHL, civilian property could be seized by reasons of military necessity.[[153]](#footnote-153)Then, the Court examined whether the security oriented-goal pursued by the construction of the barrier could have been achieved by building an alternative route that would inflict less damage to civilians; secondly, it established that the building of the fence would be disproportionate ‘if a certain reduction in the advantage gained by the original act – by employing alternate means, for example - ensures a substantial reduction in the injury caused by the […] act.’[[154]](#footnote-154) Here we can see how the principle of military necessity has to be measured against not the criterion of minimization of resource expenditure (as in the *Hostage* case), but against a choice of means approach whereby the reduction of damage caused to the civilian population plays a significant part. Despite this version of necessity cannot be simply juxtaposed to the version necessity that is applied in IHRL and the *jus ad bellum*, it represents nonetheless a restrictive application of military necessity, one which stands in stark contrast to how the principle operates in relation to the greater part of *jus in bello* norms.

### 1.4. Provisional Conclusion.

The above paragraphs have discussed the principle of military necessity and identified its function under the *jus in bello*, arguing that the principle possesses a primarily permissive function, with a restrictive function performed in those rules that expressly qualify military necessity as an exception. Other exceptional military necessity, the greatest restrictions placed on violence in armed conflict are, instead, influenced by values reflected in the so called ‘principle of humanity’. These values are therefore are external to the principle of military necessity and, by limiting (and interacting with) it, inform the fundamental provisions of the modern *jus in bello* and, most importantly, have shaped the content of the rules of targeting, which are quintessential to the regulation of hostilities.[[155]](#footnote-155)

## 2. Human Dignity and the foundations of the principle of humanity.

### 2.1. Preliminary remarks.

The principle of humanity is the main driver of the process of humanization. While the introduction of the thesis has defined its function as a normative-ideational principle that influences the norm-creation and interpretation of IHL rules, this section will discuss what its foundations are. In this regard, it must be observed that the specific content of the ‘elementary considerations of humanity’ constituting the principle of humanity has significantly evolved over time, moving forward from the purely humanitarian spirit that inspired the adoption of the First Geneva Convention in 1864, to embrace a wider meaning that is grounded in the protection of human dignity, a concept that bears a foundational role within the law of armed conflict and within international law in general.[[156]](#footnote-156) As the ICTY recognized in the *Furundzija* case judgement, ‘the essence of the whole corpus of international humanitarian law as well as humanitarian law lies in the protection of human dignity. […] The general principle of respect for human dignity is the *raison d’etre* of international human rights and international humanitarian law’.[[157]](#footnote-157) Significantly, the Furundzija dictum echoes the importance given to the idea of dignity in international law instruments such as the Universal Declaration of Human Rights or the preamble to the International Covenant on Civil and Political Rights, which recognize that human rights ‘derive from the inherent dignity of the human person’[[158]](#footnote-158), as well as in national constitutions, in which human dignity is cited as a principle having a fundamental value.[[159]](#footnote-159)

At this point, it is essential to premise that any argument related to the foundational function of human dignity within IHL cannot be dealt without reference to the emersion of the idea of human rights, which has been an influencing factor in the development of IHL, and its relationship with the notion of human dignity.Therefore, linking dignity to human rights is necessary in order to connect dignity to the principle of humanity under the *jus in bello*. In addition to this, I must clarify in which sense I am using the term ‘foundation’. At the most general level, we can say that that A is the foundation of B if the latter derives for the former. Thus, we can approach the foundational claim about human dignity from three different angles. The first is that human dignity functions as an historical basis, an approach which implies the existence of a discourse over the meaning of human dignity, which then generated, as a matter of genealogy, the idea of human rights and then informed the principle of humanity under IHL. It is not, however, possible to trace such a linear path between these concepts: as we shall see, the idea of ‘dignity’ was used since ancient times, and the concept of ‘human’ dignity was firstly introduced among the Stoic philosophers in Rome. Yet, reflections on the nature of human rights are about as old, often stemming from religious texts, while limitations on the conduct of hostilities (often based on conceptions of honour and chivalry) can also be found across different cultures. Even by restricting our inquiry to the more specific timeframe of the Modern Era, we can see how the concept of human dignity did not constitute any basis for the development of the idea of human rights. Rather, we can notice the opposite, that is, that ‘the idea of dignity reflects socio-historical conceptions of basic rights and freedoms’.[[160]](#footnote-160) Having excluded that human dignity can be the foundation of the concept of human rights on an historical basis, we can now discuss the argument that ‘the dignity of human beings is a formal transcendental norm to legitimize human rights claims.’[[161]](#footnote-161) The function of dignity, under this approach, is that of being the ultimate source of human rights norms, similarly to how a norm of constitutional rank gives validity to a hierarchically inferior norm. [[162]](#footnote-162) The major setback of this argument is that it can be counter-claimed that what gives human right norms their legitimacy is the fact that they emanate from treaties that have been signed and ratified in accordance with international law. Certainly, a possible rebuttal to the above point would be to say that the most important human right treaties have a declaratory status, rather than being constitutive of human rights. In other words, human rights treaties merely reaffirm and recognize the existence of rights that human beings already have by virtue of their dignity, which operates as an extra-legal concept that gives legitimacy and, therefore, is foundational to human rights. As such, it has been argued that the IHRL Treaties represents ‘a positive law response to suprapositive ideas’,[[163]](#footnote-163) rather than tracing back the legitimacy or validity or human right norms from non-positive law. This argument opens up to the possibility that the foundational role of human dignity with regards to the concept of human rights, as well as with regards to humanitarian considerations under IHL, can be understood in logical rather than legal terms. In other words, I believe that from the idea of human dignity we can logically deduce the existence of human rights norms, and from the existence of human rights we can give context and meaning to the principle of humanity within the *jus in bello*. Doing so, however, requires two intermediate steps. The first is an examination of how of the concept of dignity changed over time and how it became foundational to human rights norms, while the second step is to recognize the inherent limits of human rights norms for protecting human dignity in times of armed conflict.

### 2.2. Human Dignity: Evolution of the idea, from Cicero to Kant.

The origins of the idea of dignity are rooted in Roman language, where the word ‘dignitas’ was employed to signify the status a person had by virtue of possessing (or being accorded) high rank.[[164]](#footnote-164) The concept of *dignitas* was thus regarded as synonym of worthiness, associated mostly with a person’s social role, [[165]](#footnote-165) but was not merely confined to individuals, as it applied to institutions and the State itself.[[166]](#footnote-166) Since dignity expressed an elevated position within the social order, it follows that different people possessed different degrees of dignity. Certain individuals, such as aristocrats, were persons of dignity, as opposed to the common folk, who lacked dignity altogether. Yet even members of the noble class had a comparatively inferior kind of dignity than that associated with being a king.

Possessing dignity had two distinct consequences. First of all, there was a sense of esteem and deference owed to the dignitary; secondly, there was a certain social bearing connected with being a person of dignity, who was thus expected to carry himself in a way that befitted their status. Therefore, those having dignity cannot perform specific tasks and labours, nor can they marry ‘outside’ of their rank or behave in way that were deemed inappropriate. The concept of dignity as a *status* persist today, and has been incorporated in different legal systems, whereby the infringement of the dignity that is due to an individual or to an institution gives rise to civil and criminal remedies. Having said that, it is clear from the above that in its origin the concept of dignity was intended as anti-egalitarian status, the opposite of how the term is understood today, that is, as a trait inherent in all human beings.

The idea that dignity could be a common feature of humanity was firstly developed by the Stoic Roman philosopher Cicero. In *De Officis*, Cicero compared human with animals, arguing that animals were essentially driven by the need to satisfy the demands of their bodies (such as mating and providing food for themselves), whereas humans were able to engage in form of self-reflection. It is this ability to use reason that confers human beings ‘dignity’ and elevates them above the animal kingdom.[[167]](#footnote-167) During the medieval period, the idea of dignity was identified with the concept of the *imago Dei*: since man was made in the image of God, it was endowed the gift of dignity in order to distinguish him from other humans. From this theoretical background, the Italian scholar Giovanni Pico della Mirandola developed the next logical step in the evolution of the concept.

In the oration *On the Dignity of Man* (*De Dignitate Homini*), the Renaissance philosopher argued that the substance of dignity, while still being bestowed by God, was the human capacity to self-determination, that is, the ability to choose the life one wishes for: [Dignity] is given to him to have that which he chooses and to be that which he wills.’[[168]](#footnote-168)Therefore, we can see that the traditional meaning of dignity, whereby the concept was associated with intra-human social rank, had been transformed into an egalitarian status. The disparity, therefore, was no more between the noble classes and the common folk but between human beings and the rest of nature. The universalization of the idea of dignity made clear that its substance could not be a matter of hereditary or bestowed social standing but lied instead in the distinctive and unique trait that humans have to decide their own fate. While both Cicero and Pico della Mirandola were the greatest contributors in the evolution of the traditional idea of dignity, its modern meaning owes much to the work of Immanuel Kant. In the Groundwork on the Metaphysics of Moral we find this significant passage:

‘In the kingdom of ends everything has a price or dignity. What has a price can be replace by something else as its equivalent; what is raised above all price and therefore admits no equivalent has a dignity. Morality is the condition under which a rational being can be an end in itself, since only through this is it possible to be a law giving member in the kingdom of ends. Hence morality, and humanity insofar as it is capable of morality, is that which alone has dignity.’[[169]](#footnote-169)

From the above statement we can infer that the essence of dignity in the Kantian approach is not just the capacity to self-determination, a concept that was already explored, albeit to different degrees, both by Cicero and Della Mirandola, but the ability of human beings to make ‘universal law’, that is, to create a moral law that is binding upon the individual self and others. More specifically, this requires evaluating what different courses of actions are appropriate, or not appropriate, to be pursued; but that, according to Kant, is not enough to say that we have dignity. It is also necessary that, after we have decided upon something, that we bind ourselves to the decision that we made, and to pursue what we have determined ourselves to do. It is only when these two elements are both present that we are ‘normative agents’ and, therefore, that we possess dignity. In this way, this understanding of dignity can be reconciled with the traditional meaning of the concept as an elevated rank from which both a duty on the self to behave according to his social bearing, and a duty on others to treat the dignitary with respect, are derived. And we shall see how, from the Kantian interpretation of dignity as an elevated status that is owed to all human beings by virtue of their normative agency, it is possible to move closer to the contemporary meaning of the concept, where dignity is proclaimed as being the foundation of human rights and, most importantly for the purposes of the present argument, of international humanitarian law.

### 2.3. The contemporary meaning of human dignity.

When confronted with the task of understanding the contemporary meaning of human dignity, we face an apparent contradiction. On the one hand, we can see that dignity is heralded as being ‘inherent’ in all human beings, or as constituting ‘the raison d’etre’ of International Human Rights Law and International Humanitarian Law. Yet, on the other hand, we find several provisions that are aimed at ensuring that individuals are not deprived of their dignity or shall not have their dignity diminished. Thus, Art. 10 of the ICCPR states that ‘All persons deprived of their liberty shall be treated with respect of the inherent dignity of the human person’;[[170]](#footnote-170) similarly, Common Article 3 of the Geneva Convention prohibits ‘cruel treatment and torture’ and ‘outrages upon personal dignity, in particular degrading and humiliating treatment.’[[171]](#footnote-171) In light of this, one could argue that human dignity cannot be construed as the foundation of human rights and IHL if it needs to be protected by specific norms. In this regard, it can be pointed out that this dilemma can be solved by looking at the functions that the contemporary concept of human dignity performs. The first is that of a status, inherent in all humans by virtue of their normative agency, that is, their capacity to decide their own fate and to act accordingly.[[172]](#footnote-172) The possession of dignity as a status justifies certain normative demands, consisting in what treatment is expected from others (and, therefore, concerning the standard of behaviour that humans ought to live up to). The realization of these normative demands creates the conditions under which an individual might be said to have dignity. This is the second, essential function of human dignity, from which it would be possible to derive the existence of the most important human rights.[[173]](#footnote-173) This brings us to the question as to what conditions need to be in place for an individual to have human dignity. In this regard, among the many diverse interpretations of the features inherent in the idea of human dignity, James Griffin has developed a three-staged approach to the concept.[[174]](#footnote-174) According to Griffin, the first stage of human dignity is the very kernel of the idea in its contemporary meaning, what he calls ‘autonomy’, a term that is used as a synonym to normative agency. What are the conditions that must be in place in order to have autonomy? The most obvious one is that an individual must have his physical and mental integrity unthreatened by external violence. But being alive and intellectually capable to act as a normative agent, according to Griffin, is not enough to have dignity. Consider the example of an individual who has been enslaved or incarcerated. Although, in principle, he does have dignity, because he is mentally and physically able to act autonomously, in practice his human dignity and his capacity of self-determination are greatly diminished, since he lacks the freedom to act in accordance with his own determinations. Therefore, the second stage of human dignity in the account of Griffin is to have liberty, that is, to act without being restrained, physically or otherwise, by the will of others. Finally, the third stage of human dignity is the possession of a certain level of welfare with which the individual will be able to pursue what he has determined to do, such as a house, or food, education and a good level of health.

Taken together, autonomy, liberty and wellbeing constitute the conditions of dignity, that is, the state of affairs that human beings enjoy when the normative demands that are ought to them are satisfied. In this regard, we are now able to logically infer a catalogue of different human rights norms stemming from the different elements of human dignity. Thus, autonomy is ensured by the provisions protecting the right to life, such as. Art 6 of the ICCPR or Art. 2 of the European Convention of Human Rights, whereas norms prohibiting torture and degrading treatment, the prohibition of arbitrary arrest and, generally, those granting political rights all relate to liberty. Welfare, finally, is engaged in provisions related to socio-economic rights, such Art. 23 (2) UDHR, according to which ‘[e]veryone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity.[[175]](#footnote-175)

### 2.4. Human Dignity and the Limits to the applicability of Human Rights in times of armed conflict.

What emerges from the above is that we can justify the claim that human dignity can be understood as a foundation at least on a logical basis, and we notice how the dignity of the individual is guaranteed by the IHRL regime through the conferral of a corresponding set of human rights instrumental, for each individual, to the exercise of their autonomy, liberty and welfare. However, when it comes to the law of armed conflict, the protection of human dignity has taken a different path, given the contextual differences between the IHRL regime and IHL. In fact, while the *IHRL* regime protects the individual in times of peace, in which the exercise of dignity can be properly ensured in the absence of violent conflict, the application and interpretation of human right norms in times of armed conflict is limited by different factors. First, human rights treaties normally apply with respect to individuals within the territory of the State and their jurisdiction. The two terms are not strictly interchangeable with one another: this means that human right norms would be applicable, even outside the territory of a State, should the latter exercise jurisdiction over an individual. In this regard, the boundaries of the concept of ‘jurisdiction’ are limited to situations in which the State agents exercise ‘effective control and authority’ over a person,[[176]](#footnote-176) as well as in situations of stable occupation.[[177]](#footnote-177) While it is beyond the scope of this research to further elaborate on the matter,[[178]](#footnote-178) what is relevant is that States will be bound to apply human rights treaties in situation of non-international armed conflicts (that is, armed conflicts taking place within their territory), whereas, in the case in which the State is participating in an international armed conflict taking place outside its territory, human rights obligation will trigger only if the conditions for their extra-territorial application are met. Moreover, human rights treaties contain clauses whereby the applicability of their norms can be derogated in times of ‘public emergency threatening the life of a nation’ like an armed conflict. Even with respect to those rights which are not subject to derogation, such as the right to life, they must be interpreted in accordance with *jus in bello* rules. In this regard, the relationship between IHRL treaties and IHL has clarified by the ICJ in the *Nuclear Weapons* Advisory Opinion, where the Court addressed the question of whether the use of nuclear weapons in war time could constitute a violation of Art. 6 of the International Covenant on Civil and Political Rights, according to which ‘every human being has the inherent right to life. […] No one shall be arbitrarily deprived of his life.’[[179]](#footnote-179) The Court noted that the protection of the ICCPR does not cease in times of armed conflict, except ‘by operation of the derogation clause under Art. 4 of the Covenant. After having pointed out that no derogation is admitted with regards to the right to life, the Court stated that:

 ‘the test of what constitutes an arbitrary deprivation of life, however, then falls to be determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities. Thus whether a particular loss of life, through the use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to Article 6 of the Covenant, can only be decided by the law applicable in armed conflict *and not deduced from the terms of the Covenant itself*.*’[[180]](#footnote-180)*

The Court pronounced itself over the nature of the relationship between the two legal regimes again in the *Wall Case*, where it held that three possible situations might occur:

‘[s]ome rights may be exclusively matters of international humanitarian law; other may be exclusively matters of human rights law; yet others may be the matters of both these branches of international law. […] The Court will have to take into consideration both these branches of international law, namely human rights law and, as *lex specialis*, international humanitarian law.’[[181]](#footnote-181)

The focus of these statements from the ICJ is on the *lex specialis* principle, a term of Latin origin that describes the hierarchical relationship between two norms or legal regimes, whereby the more specific rule applies *in lieu* of the more general rule. The *lex specialis* principle is, in other words, a method of norm conflict resolution and avoidance: this means that a right such as the right to life, and the protection of human dignity that it affords to every individual, must be interpreted in light of the principle of distinction, whereby is lawful (and therefore non-arbitrary) to deprive a combatant of their life, whereas the intentional targeting and killing of civilian is not. The limits on the applicability and interpretation of human rights norms do not mean, however, that human dignity in armed conflict shall not be protected. Rather, this task is performed by the principle of humanity, which ensures that the normative demands constituting the conditions on which dignity can be exercised are nonetheless ensured to the greatest extent possible.

## 3. The dynamic between the human dignity and military necessity within the law of targeting.

What can rather be observed in IHL is that the concept of human dignity acts as a counterbalancing principle to that of military necessity, both in the process of norm creation and interpretation of the rules of the *jus in bello*, as premised in the Introduction. As a result, we shall see that the protection of human dignity in IHL diverges from the IHRL regime in two main regards: firstly, it is conditional on the status on the affected individual, as opposed to IHRL where the protection of human dignity is owed to every person; secondly, while human rights rules are interpreted to ensure protection to all the constitutive elements of human dignity, IHL norms provide a lower quantumof protection. This difference in approach can be observed by examining the rules on ‘targeting’, that is, the set of provisions that regulate the amount of violence that combatants may lawfully employ in warfare. As will be discussed below, they represent the area of IHL where the tension between the permissive principle of military necessity and the constraining effect of human dignity-based considerations is most evident.

### 3.1. The principle of distinction between civilians and combatants.

The principle of distinction is embodied in Art. 48, according to which:

‘In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.’[[182]](#footnote-182)

The principle is considered the cornerstone of the rules of targeting, and its relevance has been reaffirmed multiple times by international courts and tribunals. In the *Nuclear Weapons Advisory Opinion*, the ICJ stated that the principle of distinction ‘is one of the cardinal principles contained in the texts constituting the fabric of humanitarian law… [and one of the] intransgressible principles of customary law.’[[183]](#footnote-183) The ICTY recognized the customary status of the principle of distinction in several cases,[[184]](#footnote-184) most notably in *Strugar*,[[185]](#footnote-185) where the Appeals Chamber noted that the prohibition on attacking civilians is part of customary international law, and a violation of this principle entails individual criminal responsibility. In a similar vein, in the *Tablada* case, the Inter-American Commission on Human Rights (IACiHR) affirmed:

‘In addition to Common Article 3, customary law principles applicable to all armed conflicts require the contending parties to refrain from directly attacking the civilian population and individual civilians and to distinguish their targeting between civilians and combatants and other lawful military objectives. ‘[[186]](#footnote-186)

At the basis of the principle of distinction is the dichotomy between the categories of civilian/combatant and civilian object/military objectives, which represent the two sides of the balance between human dignity and military necessity considerations.

#### 3.1.i. The distinction between civilians and combatants.

The *rationale* of the distinction between civilians and combatants is that exists a military necessity to kill and/or capture combatants, who have forfeited the right not to be killed by engaging in acts of violence, thus contributing to the existence of an armed conflict. [[187]](#footnote-187) Without any fighting, there would be no need to engage in violent activities that are military necessary to bring about the end of the war. At the same time, however, the law of armed conflict accords them the status of combatant, which entails the right to lawfully participatein an armed conflict, the primary consequence of which is that of being granted, upon capture by the enemy, the status of Prisoner of War (POW).Here we can see that human dignity considerations are, on the one hand, greatly overshadowed by demands of military necessity as far as protecting the life of combatants is concerned, since they can be lawfully made the object of an attack, and therefore killed. Yet, on the other hand, a modicum of protection of their dignity is ensured by the provision of POW status-related rights, whereby POWs cannot be prosecuted by taking part in hostilities, must be treated humanely in all circumstances, have the right to a certain standard of accommodation, food, hygiene and medical care while detained, and must be released and repatriated upon the end of hostilities. Conversely, civilians do not engage in fighting and, therefore, there is no causal link between the existence of an armed conflict and their actions: as a result, considerations related to human dignity are strongly focused on protecting the life and the physical integrity of the individual civilian, since they are two of the conditions by which autonomy and liberty can be exercised, and those that are most likely to be affected by violence in armed conflict. This form of protection consists, essentially, in the general prohibition on attacks against the civilian population under Art. 51 API[[188]](#footnote-188), and in several more specific provisions, such as Common Article 3 of the Geneva Conventions, which forbids ‘outrages upon personal dignity, humiliating and degrading treatment.’[[189]](#footnote-189). Similarly, Articles 75 and 85 of Additional Protocol I includes enforced prostitution and apartheid among the practices against human dignity.[[190]](#footnote-190)

 At the level of norm-creation, the balance between the military necessity oriented consideration that combatants are liable to be killed and wounded, and the idea that civilians enjoy protected status, is achieved by defining the notion of civilian in a negative way: a civilian is a non-combatant, a category that includes also individuals who have been put *hors de combat*.[[191]](#footnote-191) In turn, the notion of combatancy is partly qualified by membership of the armed forces of a State or an armed group,[[192]](#footnote-192) and partly qualified by the notion of ‘direct participation in hostilities’ (‘DPH’). With regards to the latter, Art. 51 of Additional Protocol I mandates that ‘civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities’.[[193]](#footnote-193) The notion of DPH has been the object of a study by the ICRC, which resulted in the *Interpretive Guidance on the Notion of Direct Participation in Hostilities* and can be summarized as follows: when a civilian is engaged in the preparation or performance of acts that meet a certain threshold of harm and which are directed against one of the Parties to a conflict or in support to a Party to a conflict, he is directly participating in hostilities, making him lose his non-combatant immunity.[[194]](#footnote-194) As a consequence, a civilian can be lawfully targeted, and killed, but only as long and for such time as his direct participation endures: when the activities amounting to a direct participation in hostilities cease, the individual retains his civilian status and the protection from attack that is attached to it.

While the elements of DPH will be discussed in a following chapter, what is important to underline is that the notion of DPH represents the other side of the coin of the civilian-combatant dualism, and is rooted in the consideration that, as long and for such time as a civilian makes a causal contribution to the armed conflict, he is no longer innocent but has the same legal standing of any other combatant, and for this reason their dignity might be lawfully violated, by making them the target of an attack. The notion of DPH represents, then, the attempt to introduce a balance between military necessity and human dignity considerations, in cases where it is not possible to rely on membership of the armed forces of a State or a non-State armed group as the only requirement for the attribution of combatant status. In this regard, the notion of DPH has been the subject of intense critiques, focused especially on the interpretation of the temporal requirement of the concept. In this regard, Michael Schmitt has argued that if a civilian can only be targeted ‘for such time as’ he is directly participating in hostilities, the result is that of creating a ‘revolving door’, since ‘[A] civilian direct participant who conducts recurring operations against the enemy would only be targetable during the period from the time of departure until return. Between operations, the direct participant could not be attacked’.[[195]](#footnote-195) As a consequences of this, combatants of the armed forces of a State would be placed at a serious disadvantage, considering that they can be attacked at all times.[[196]](#footnote-196) Similarly, Boothby has noted that the interpretation of the ICRC on the scope of DPH, specifically the way in which the elements of preparation, deployment, and return were interpreted was too narrow.[[197]](#footnote-197) Despite the fact that these critiques have been addressed by the ICRC on a number of occasions, [[198]](#footnote-198) they are interesting in that they show an interpretation of the law that privileges military necessity over human dignity-inspired considerations, and they reflect how finding a balance between the two principles is bound to remain a difficult task.

#### 3.1. ii. The distinction between Military Objectives and Civilian objects.

Art. 52 AP I provides that ‘civilian objects shall not be the object of attack or reprisals’ and that ‘attacks shall be limited strictly to military objectives.[[199]](#footnote-199). In order to qualify as a military objective, an object must, by its nature, location, purpose or use, ‘make an effective contribution to military action’ and, secondly, its ‘total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage’.[[200]](#footnote-200)

The requirement that an object must make an ‘effective contribution to military action’ means, essentially, that not only military-related buildings, installations, weapons can be targeted (nature), but any other object by virtue of its actual use, future use (purpose) or location, therefore implying that an object which is civilian by nature can nevertheless be targeted. In modern warfare, this sub-requirement has a profound impact on the conduct of hostilities, as several objects are, in fact, ‘dual-use’: electrical grids and power plants, telecommunication networks, roads and bridges are civilian objects in nature but can qualify as a military objective under the criteria of effective contribution to military action (for instance, by being used by the military).

But the former requirement is not sufficient for meeting the threshold of military objective set out by Art. 52 (2) AP I, as there must be a nexus of causal proximity between the targeting of a military objective and gaining a definite military advantage – that is, getting one step closer to the submission of the enemy.

We can see here how the *rationale* behind the distinction between the categories of ‘civilian object’ and ‘military objective’ flows from the same logic that mandates the distinction between ‘civilian’ and ‘combatant’ found in Art. 51, in the sense that it aims to protect the dignity of the civilian population beyond the sphere of physical integrity, to include objects and that are significant to the welfare of the civilian population, such as houses, hospitals, food production facilities and so on. The only difference between the two provisions is in the semantics, since the requirement of causal contribution to war is broken down into the concepts of ‘effective contribution to military action’ and ‘definite military advantage’, instead of ‘membership in the armed forces of a State or an armed group’ and ‘direct participation in hostilities’.

### 3.2. The Principle of Proportionality.

The principle of proportionality represents the logical corollary of the principle of distinction, and can be deduced from the prohibition to indiscriminate attacks found in Art. 51 (5) (b) of AP I. The wording of the provision specifies that an indiscriminate attack is one that ‘may be expected to cause incidental loss of 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’.[[201]](#footnote-201)

The assumption behind the military necessity – humanity dynamic of the principle of proportionality stems from the ramifications of the doctrine of double effect (DDE), [[202]](#footnote-202) according to which, under certain circumstances, incidental harm caused to civilians and civilian objects is permissible if the attack that caused was necessary to achieve some proportionate good. Hence, we can assume that a combatant is justified for an attack that violates the dignity of the civilian population, by resulting in death or physical injury, if the combatant does not intend to deliberately attack civilians, as it would be in plain violation of the principle of distinction. Instead, the attacker must take inconsideration that death or injury to civilians might occur as a side-effect of an attack that is taken for the achievement of a military advantage and weigh one against the other. Reframed in terms of the dynamic between human dignity and military necessity, this means that military necessity allows a combatant to violate the dignity of the civilian population only insofar as if it is the result of an attack which has been intentionally directed against a lawful target, and provided that the expected harm caused to the dignity of the civilian population does not disproportionately exceed the military advantage anticipated from the attack. That having being said, it is however extremely difficult to pinpoint where the line must be drawn between the two competing principles: should a soldier avoid launching an attack against a school used as an ammunition deposit if it would violate the dignity of civilians in a significant manner, by causing widespread injury, destruction and by depriving students of their education? Would the answer be any different if the civilian lives would be weighed against the life of a high-ranking military official? From the wording of Art 51 (5) (b) no guidance is provided for answering such questions and weighing human dignity considerations against military necessity must inevitably be assessed on a case-by-case basis. In this regard, the relationship between human dignity and military necessity can be further appreciated by looking at the rules on precautions in attack, since they flow from the same *rationale* of protecting the dignity of the civilian population by minimizing harm resulting from attacks.

### 3.3. The Rules on Precaution in Attack and against the effects of attack.

The principle of precaution under Art. 57 AP I requires combatants to take constant care to spare the civilian population, civilians and civilian objects from the dangers of military operations. As such, it provides a series of specific obligations, including taking ‘all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and civilian objects’;[[203]](#footnote-203) refraining to launch,[[204]](#footnote-204) cancel or suspend an attack which appears to be indiscriminate;[[205]](#footnote-205) finally, ‘when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.’[[206]](#footnote-206) At first glance, the wording of Art. 57 suggest that strong human dignity considerations have priority over military necessity reasons, since combatants are required to do anything feasible to avoid or minimize collateral damage when launching their attacks. However, a closer analysis may yield a different conclusion. In this regard, the key element of the provision is the notion of *feasibility.* As we shall see in more detail in Chapter 6, it is a concept influenced by several factors, among which there is the increased risk on the attacking forces should they choose the attack that avoids or minimizes collateral damage. In this regard, it might be possible that a less harmful option of attack may be considered ‘unfeasible’, if there is an alternative, more harmful option in which increased collateral damage is justified by a reduction in the risk faced by the combatant.[[207]](#footnote-207) To put it more succinctly, it can be argued that a combatant must not put himself in greater danger to reduce collateral damage to the civilian population. Consequently, we can see how in certain circumstances the permissive nature of military necessity would prevail over the dignity-driven obligation to avoid or minimize collateral damage. A similar conclusion stems from an analysis of Art. 57 (3) AP I, which requires combatants to choose the attack that causes the least collateral damage, but only when a choice is possible between several military objectives for obtaining a similar military advantage. This has an important consequence, because if a choice between two different attacks is possible, and one provides a greater military advantage than the other, the obligation to choose the attack causing the least damage does not arise: therefore, it can be argued that Art. 57 (3) allows combatants to ‘inflict any quantum of additional harm to civilians […] provided doing so requires some additional quantum of military advantage.’[[208]](#footnote-208) It appears, then, that under these specific provisions of Art. 57 AP I the balance is tilted towards military necessity considerations, the only exception being Art 57 (2) (a) (iii) and Art.57 2 (b), which mandates combatant to refrain of cancelling an attack when such attack would be indiscriminate and, therefore, contrary to the principle of distinction.

The rules on precautions in attack are complemented by Art. 58, which provides a series of measures that parties to the conflict must take against the effects of attacks, consisting in the obligation to everything feasible to segregate military objectives from civilian objects and endeavour to remove the civilian population and objects from military objectives. In this regard, the same considerations made with regards to Art. 57 apply to the rules of precautions against the effects of attacks. While human dignity-based considerations are certainly present, they are greatly mitigated by the fact that the obligations set forth by Art. 58 are subject to the discretionary requirement of feasibility, which leans towards the demands of permissive military necessity.

### 3.4. The Principle of Unnecessary Suffering.

The principle of unnecessary suffering is considered an ‘intransgressible’ principle of the *jus in bell*o,[[209]](#footnote-209) and is closely connected to the rules on targeting since it provides additional restriction on the amount of violence that can be lawfully exerted in the battlefield. According to Art. 35 AP I, ‘it is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering’, because ‘the right to the Parties to the Conflict to choose methods or means of warfare is not unlimited.’[[210]](#footnote-210) The principle of unnecessary suffering was formulated firstly in the St. Petersburg Declaration and, three decades after, in The Hague Convention on the Laws and Customs of War on Land, hence, within the codification period which I referred to as ‘The Hague Law’, where the category of ‘civilian’ was largely unregulated, and human dignity considerations, albeit few, were centred on the protection of combatants. The combatant-centred nature of the principle stems from the fact that no intentional violence can ever be inflicted on civilians, therefore it would be redundant to prohibit suffering which is ‘unnecessary’ and injury which is ‘superfluous’. Thus, we can see how the protection of the dignity of combatants operates in the sense of restricting the quantum of violence inflicted against combatants only to that which is *necessary* to disable them, and no further. Examining Art. 35 AP I, it distinguishes between means and methods of warfare. With regards to the latter category, it concerns primarily the law of weaponry and has had an impact of the codification of this segment of the *jus in bello,* resulting in the ban of poisonous weapons,[[211]](#footnote-211) asphyxiating gasses,[[212]](#footnote-212) blinding lasers weapons, [[213]](#footnote-213)anti-personnel mines[[214]](#footnote-214) among other categories of weapons that are deemed to uselessly aggravate the suffering of combatants when employed in the battlefield. It can then be assumed that the protection of combatants’ dignity *qua* humans is an important factor in the law of weaponry. That said, it must be however noted how the law of weaponry does not impact directly on the rules of targeting, as opposed to the prohibition on the employment of‘methods of warfare’, which is more closely connected with the *quantum* of force to be used *vis-à-vis* combatants. An analysis of the principle of unnecessary suffering, as applied to methods of warfare, shows that it has a narrow scope of application. Consider, for instance, that the prohibition on starvation as a mean of warfare under Art 54 (1) AP I applies only to the civilian population,[[215]](#footnote-215) whereas combatants can be starved to death as no amount of suffering would be militarily un-necessary: yet, it is clear that starving combatants to death violates their dignity. It is easy to see where the edge of the balance between what is ‘humane’ and what is military necessary falls in this situation. A recent attempt to shift the balance has been made by ICRC’s *Guidance* under section IX, titled ‘Restraint on the Use of Force in Direct Attack’, which reads as follows:

‘In addition to the restraints imposed by international humanitarian law on specific means and methods of warfare, and without prejudice to further restrictions that may arise under other applicable branches of international law, the kind and degree of force which is permissible against person not entitled to protection against direct attack must not exceed what is necessary to accomplish a legitimate military purpose in the prevailing circumstances’.[[216]](#footnote-216)

The rationale of Section IX owes much to a quote by Jean Pictet, whereby ‘if we can put a soldier out of action by capturing him we should not wound him, if we can obtain the same result by wounding him, we must not kill him, if there are two means to achieve the same military advantage we must choose the one which causes the lesser evil.’[[217]](#footnote-217) The implications of this statement are far reaching: if applied to the *lex lata,* combatants would have to evaluate the necessity to kill an enemy combatant where other, least-harmful options are available. Scholars like Ryan Goodman and Nils Melzer, who favour this view, argue that ‘it would defy basic notions of humanity to kill an adversary…when there is manifestly no necessity to do so.’[[218]](#footnote-218) Conversely, opponents of this reading point out that the ICRC’s position is a misapplication of the law,[[219]](#footnote-219)is rejected by State practice and cannot constitute *lex lata*,[[220]](#footnote-220)and would place an unreasonable burden on combatants. If anything, the debate surrounding Section IX of the DPH Guidance demonstrates the practical problems in finding an adequate equilibrium between the two competing principles of humanity and military necessity. In fact, while considerations of military necessity push towards giving belligerents a great degree of discretion in the amount of violence that they can inflict upon combatants in order to achieve their military objectives, the principle of humanity strives for the opposite goal, that of protecting the dignity of combatants by restricting the *quantum* of violence that they may be subjected to.

Having exemplified how the principle of unnecessary suffering is connected to the process of humanization and the dynamic that lies therein, this thesis will not devote further discussion on the topic (with the exception of the conclusion).

## 4. The emergence of cyberwarfare: challenges and opportunities for humanizing the law of targeting.

The previous sections have highlighted the interpretive issues underlying the relationship between military necessity and the protection of human dignity in the context of the rules on targeting. In the opinion of the present writer, such problems are inherently related to the changing nature of modern conflict. Since the end of WWII, the world witnessed a transition from the ‘traditional’ form of international armed conflict, fought between sovereign States, to non-international armed conflicts, where a State engages in a military confrontation against one or more non-state armed groups.[[221]](#footnote-221) As the result of this ‘civilianization’ of warfare’, hostilities often take place within densely populated urban areas, and the participation of irregular troops and civilians who are participating in hostilities is a common reality. Under these circumstances, it is extremely problematic to interpret the rules on targeting to accommodate reasons of military necessity with the goal of protecting the dignity of the civilian population and persons *hors de combat.*

In this context, the rise of cyber technology and their deployment in military operations adds an additional layer to the complexity of modern warfare. Several peculiarities make cyber weapons unique. One is the dimension in which they exist: as opposed to conventional forms of warfare, where the scope of the battlefield is limited to the territorial reach of the weapons employed, cyber weapons operate primarily in cyberspace. Travelling through cyberspace, cyber-attacks can be launched from remarkable distances and can reach their target (usually the computer system or network of an enemy) within the blink of an eye: this is problematic for the *jus in bello,* a body of law that was progressively formed to regulate activities taking place in a physical, geographically limited battlefield, as opposed to a virtual one. The unique features of cyber weapons become even a greater issue considering that they can generate effects in a way that can be both similar to conventional weapons and, at the same time, completely unprecedented compared to traditional means of warfare. Usually, a weapon generates physical violence by producing kinetic force, which in turn causes death or injury to individuals and damage or destruction to objects. Cyber-attacks are certainly capable of causing physical violence: a computer virus can disable a train in a crowded station and can derail it; an intruder can gain control of the operating system of a dam and release its gates with the intention of causing massive floods, and so on. However, we have seen how cyber weapons can be used in a more malicious, but no less devastating way: they can disable an electrical power plant and deprive urban area of electricity, or they can strike down the economy of a State by manipulating its stock market. In these scenarios, there is no causation of violence in its *physical* sense, yet the consequences are as serious as the causation of death of individuals or destruction of objects. Under these circumstances, determining when the principle of distinction and the principles of proportionality and precaution should be applied becomes not only increasingly difficult, but yields dramatically different results according to the interpretation one has to adopt. In this regard, it must be underlined that cyber-warfare capabilities can be employed for reducing the sum total of suffering caused in an armed conflict. The virtuality and remoteness of cyber weapons may signify that cyber-combatants are subject to a lesser level of threat to their physical integrity when launching cyber-attacks, and this could potentially lead to a different interpretation of the proportionality principle, one in which military necessity considerations are downplayed and the notion of ‘direct military advantage’ is interpreted narrowly, without taking into account the reduced risk for a combatant’s life. On the other hand, the use of cyber weapons can favour the emergence of a least-harmful mean approach, with p positive implications for increasing the protection of the civilian population. Considering this, the purpose of the following chapters is to discuss whether (and how) the rules on the law of targeting can be applied to cyber-operations employed in the conduct of hostilities, using a human-dignity oriented framework, in order to further promote the protection of human dignity in armed conflict and ensure the objective of reducing the violence generated by cyber-weapons. This task is therefore twofold: first of all, it demands an adaptation of the definition of attack and the underlying notion of *violence* that revolves around it. Secondly, the focus will shift on the applicability of the rules on targeting to cyberwarfare and how it affects the relationship between humanity and military necessity. In particular, considering the unique features of cyberwarfare, I will enquire if a different dynamic between the two principles is possible, and whether that military necessity considerations can further be limited by a more human-dignity oriented interpretation of the relevant rules on targeting, without depriving them of their effectiveness.

# Chapter 2. The notion of ‘attack’ in the cyber domain: towards a human dignity-oriented interpretation.

The objective of this Chapter is to develop an interpretation of the notion of cyber-attack which is consistent with the overall purpose of protecting human dignity in armed conflict. In order do to so, my argument is structured as follows: Section I will examine the definition of attack under IHL, with

an emphasis on the underlying notion of violence and its relationship with human dignity. Section II analyses the notion of cyber-attack in its different components and provides a critique of the main interpretive approaches to the notion, demonstrating why they are inconsistent with the objective of balancing military necessity considerations with human dignity. Section III introduces a human-dignity oriented interpretation of the notion of cyber-attack. Section IV provides a conclusion.

## 1. The definition of attack under the *jus in bello*.

Attacks are defined by Article 49 API as ‘acts of violence against the adversary, whether in offence or defence’[[222]](#footnote-222). To deduce the meaning of violence within Art. 49 it is necessary to apply the rules of interpretation of the Vienna Convention of the Law of Treaties (‘VCLT’). According to Art. 31 VCLT, a treaty ‘shall be interpreted in good faith, in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose.’[[223]](#footnote-223)

The concept of violence has a multi-faceted dimension and can be subject to widely diverging definitions. The Oxford dictionary interprets violence as ‘the deliberate exercise of physical force against a person, property, etc. physically violent [behaviour] or treatment; [Law] the unlawful exercise of physical force, intimidation by the exhibition of such force’.[[224]](#footnote-224)

At the opposite side of the spectrum is the approach adopted by the World Health Organization (WHO) according to which violence is ‘physical force or power […] which either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation.’[[225]](#footnote-225) Given that it’s not possible to determine the ordinary meaning of the notion of violence, resort must be had to other means of the interpretation, such as the context in which the term ‘violence’ is found. Consider, for instance, Art 54, which protects ‘object indispensable to the survival of the civilian population’.[[226]](#footnote-226) The centre of the prohibition lies in the attack, destruction or removal of objects indispensable for the survival of the civilian population; similarly, Art. 55 AP I protects the natural environment against ‘widespread, long-term and severe damage’.[[227]](#footnote-227) A similar interpretation emerges from Art. 51 API, which defines a military objective as an object whose ‘capture, destruction or neutralization’ offers a definite military advantage.[[228]](#footnote-228)A similar interpretation of violence is the focus of the prohibition to launch indiscriminate attacks, which applies to acts which are expected to cause ‘incidental loss of life, injury to civilians, damage or civilian objects, or a combination thereof, which would be excessive in relation to the concrete military advantage anticipated’,[[229]](#footnote-229) a reference that occurs in Art. 57 AP I, which defines the principle of precaution in attack.[[230]](#footnote-230)

From a contextual reading of API, it can be deduced that the drafters of the Protocol endorsed a narrow reading of the notion of violence, which must be interpreted as *physical violence*, that is, death or injury to individuals and damage or destruction to objects. However, this term should not be considered merely as a synonym of kinetic force, given that nuclear, bacteriological or chemical force are traditionally understood as constituting physical violence. In fact, as noted by Schmitt, the rationale underlying Art. 49 is centred upon the *effects* caused by an act, not by its nature: in other words, an act must cause physically violent consequences to be qualified as an attack for the purposes of *IHL*.[[231]](#footnote-231) This interpretation of violence applies not only to first-order effects, which are those that are directly consequential to an attack, but also to second-order effects, consisting in the consequential damage stemming from first-order effects. If second-order effects result in death or injury to individuals or damage or destruction of objects they fall under the meaning of violence under Art. 48 AP I. The *jus in bello* has taken into account the possibility of consequential damage in provisions like Art 56 AP I, which prohibits attacks against installations containing dangerous forces, since ‘severe losses among the civilian population may result’.[[232]](#footnote-232) Here, the focus of the Art. 56 is not on the first order effects of the attack, which will always result in the destruction or damage of a civilian object, but especially on preventing that death and injury to civilian may take place as a second order effect of such attack.

How does this interpretation of violence fit within the dualism between the principle of military necessity and the need to protect human dignity? A physically centred approach is consistent with the type of warfare that existed at the time when the Additional Protocols to the Geneva Conventions were drafted, when kinetic attacks were the primary mean by which belligerents could achieve their military objectives. Thus, attacks are acts that are necessary in a military sense, and the performance of such acts is one of the elements from which is possible to deduce, *inter alia,* the notion of combatancy and direct participation in hostilities. Furthermore, since attacks are acts of physical violence, they are capable of having an adverse impact on the dignity of the civilian population. Firstly, they can diminish the physical integrity of civilians by resulting in injury or death, thereby compromising their liberty and autonomy; or they can also affect the civilians’ welfare by destroying objects that provide for their basic needs, such as health system, food crops, shelter or housing. It follows, then, that attacks must be regulated by the principles of discrimination, proportionality and precaution, in order to limit their impact on the civilian population and objects. As we shall see, however, a definition of attack that is exclusively focused on the causation of physical violence cannot be efficiently applied to the emerging phenomenon of cyber warfare, due to its peculiar characteristics.

## 2. The notion of Attack in the context of cyber operations: preliminary considerations.

Before discussing the issue, it is worth reminding that according to the US Joints Chief of Staff, a cyberattack is any ‘operation designed to disrupt, degrade, deny or destroy information resident in a computer system or network, or the systems and networks themselves’.[[233]](#footnote-233) The definition of the US Joints Chief of Staff, further from possessing any legal value, is however useful in order to understand that cyber-attacks operate in the virtual dimension of cyberspace, by affecting *digital data* stored in a computer system or in a network. In this regard, digital data is the graphic representation of information stored in a computer network or in a computer system, and can be distinguished between ‘content-level’ and ‘operational’ or ‘context-level’ data.[[234]](#footnote-234) The former category includes the ‘surface’ content of files accessible through a computer network or system, such as the text of an article, the contents of medical databases and a library catalogue. [[235]](#footnote-235) On the other hand, operational-level data is the essential component of operating systems and software application within computer network or systems. As noted by Dinniss, operational-level data can be seen as ‘the soul of the machine. Is this type of data that gives hardware its functionality and perform the tasks we require.’[[236]](#footnote-236) While the concept of *data* will resurface in several parts of the thesis, for now it is sufficient to point out that cyber-attacks, by affecting digital data, produce effects in cyberspace which then may, or may not, result in some sort of effect in the physical world. It is then useful to distinguish these effects between first order (or ‘direct’ effects) and second-order (also known as ‘indirect’ or ‘reverberating’ effects). First order effects take place, in the chain of causation, as ‘the immediate, first order consequences of an attack, unaltered by intervening events or mechanisms.’[[237]](#footnote-237) Conversely, indirect effects are ‘the delayed and displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms’[[238]](#footnote-238).

Therefore, while first-order effects of cyber-attacks only take place in cyberspace, second-order effects manifest themselves into the physical world in several ways. Consider, for instance, the following four examples:

1) A CNA targeted the control system of two Iranian oil pipelines, causing an explosion that results in the death of two workers, employed in a nearby facility.[[239]](#footnote-239)

2) Discovered in 2010, the ‘Stuxnet’ worm successfully infiltrated within the operating systems of the turbines responsible for the uranium-refinement process at the nuclear facility of Natanz, Iran, resulting in the physical damage of a thousand centrifuges.[[240]](#footnote-240)

3) In 2007, a group of pro-Russian hacktivists called Nashi (Youth) launched a coordinated campaign of DDOS attacks against Estonia, targeting the websites of the Estonian Parliament, as well as banks and newspapers.[[241]](#footnote-241)

4) It has been alleged that in 2016 North Korean State-sponsored hackers fraudulently instructed the SWIFT system to transfer funds amounting to 1 billion $ from the Bangladesh Bank to private accounts in Sri Lanka and the Philippines.[[242]](#footnote-242)

5)A ransomware attack similar to WannaCry or NotPetya targets thousands of computer systems within a single State, blocks the access to the systems and encrypts personal data, asking for a payment to be made by each user so that they can gain access to their systems and control over their data.

In all the above scenarios, the common denominator is the first order effects stemming from the interaction between the malicious code and the digital data of the computer network or systems which it infiltrated. Rather, what differentiates them from one another is the nature and intensity of the second-order effects caused by the different cyber-operations. Thus, determining where to draw the line between cyber-operations that meet the definition of ‘violence’ under Art. 49 and those which do not has a profound impact to the conduct of hostilities and, therefore, for the protection of the civilian population.

### 2.1. Cyber-attacks as physical violence: The Kinetic Equivalence Effect test.

In this regard, I will firstly examine the definition of cyber-attack modelled after the approach of the Tallinn Manual, it is the most authoritative attempt at defining what a cyber-attack is under the *jus in bello*. Rule 30 of the Manual defines a cyber-attack 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’.[[243]](#footnote-243) This definition must be interpreted to include any consequential damage caused by a cyber-attack, as noted by the commentary to Rule 30, according to which:

“The word cause in this Rule is not limited to effects on the targeted cyber system. Rather, it encompasses any reasonably foreseeable *consequential* damage, destruction, injury, or death. Cyber-attacks seldom involve the release of direct physical force against the targeted cyber system; yet they can result in great harm to individuals or objects. For example, the release of dam waters by manipulating a SCADA system would cause massive downstream destruction without damaging the system. Were this operation to be conducted using kinetic means, like bombing the dam, there is no question that it would be regarded as an attack. No rationale exists for arriving at a different conclusion in the cyber context.” [[244]](#footnote-244)

The Manual*’*s approach analogizes the effects of cyberattacks to those caused by conventional weapons, in what has been referred to as the ‘kinetic equivalence effects test’ (‘KEE Test’) [[245]](#footnote-245): to the extent that the second-order effects of a cyber-attack result in physical violence, in the form of death or injury to individuals or damage or destruction to objects, the operation that originated them is an attack for the purposes of IHL. This does not, however, mean that any form of injury or destruction of object would necessarily, in the Tallin Manual’s approach, suffice for qualifying a cyber-operation as an attack for the purposes of Art. 49 AP I. Rather, the Commentary alludes to a certain threshold of intensity, as a’ *de minimis* damage or destruction does not meet the threshold of harm required by this Rule’.[[246]](#footnote-246) Conversely, the accompanying commentary notes that ‘non-violent operations, such as psychological cyber-operations or cyber espionage, do not qualify’ as such[[247]](#footnote-247). One divisive matter relates to what amounts to ‘damage’ to objects, and if disrupting the functionality of an object through deletion or manipulation of *digital data* is sufficient to characterize a cyber-operation as an attack.

In this regard, it must be pointed out that the *Manual* does not consider data as an object. As illustrated by the Commentary to Rule 38, ‘[T]he majority of the International Group of Experts agreed that the law of armed conflict notion of objects should not be interpreted as including data.’[[248]](#footnote-248) The explanation given by the Manual is that ‘*Data* is intangible and therefore neither falls within the ordinary meaning of the term object nor comports with the explanation of it offered in the ICRC Additional Protocols Commentary’,[[249]](#footnote-249) according to which an object is something that is ‘visible and tangible’.[[250]](#footnote-250) Therefore, according to the Manual, a cyber-operation that deletes digital data qualifies as an attack if it requires ‘physical replacement of the components’ of the system whose functionality has been compromised (the so-called functionality test). For instance, a cyber-operation that targets the computer-based distribution system of an electrical power grid would be considered as an attack if the control systems of its vital components must be manually replaced.[[251]](#footnote-251) *Vice versa*, a cyber-operation that requires mere digital data restoration does not qualify as an attack,[[252]](#footnote-252) since it does not reach the threshold of causing physical violence because no ‘damage’ or ‘destruction’ to physical objects occurs.

Having clarified this, we turn now to the application of the KEE test to the examples mentioned in paragraph 2.1. Regarding Scenario 1, the cyber-operation would be qualified as an attack under Art. 49 AP I, as its second-order effects result in damage to objects and death or injury to individuals, falling comfortably within the definition of violence explained above. A similar conclusion can be drawn with regards to Scenario 2, in which case there is no death or injury to individuals, but damage to physical objects, since the functionality of the affected turbines had to be restored by manual replacement or repairment of their physical components. In the case of Scenario 3, lacking any injury to individuals or damage to objects as a second-order effect, the cyber operation is not an attack.[[253]](#footnote-253) The fourth scenario is where the application of the KEE test becomes problematic. While it seems clear that no direct physical damage results from the cyber-attack – since the operation consists merely in the manipulation or alteration of digital data – and no death or destruction would occur as a second-order consequence, the cyber-attack would still cause serious consequences for the civilian population, especially in the form of economic damage and mental suffering. Analogous considerations can be drawn from Scenario 5, where no physical damage of a significant nature resulted from encrypting personal data, yet it seems undisputable to argue that the operation had a negative impact on the wellbeing of the affected individuals. Interestingly enough, a possible (albeit indirect) line of defence of the KEE test would be to argue that a ransomware attack like NotPetya or WannaCry would be prohibited under IHL because (and insofar as) they targeted personal medical records, which can be considered as a specific category of protected objects which must be ‘respected and protected and, in particular, not made the object of a cyber-attack.’[[254]](#footnote-254) Regardless of the fact that the KEE test would not consider a ransomware attack against medical data as an attack, the cyber-operation would be still considered unlawful. While this shows that the Tallinn Manual’s approach is more nuanced than it initially appears, I however believe it is too selective and does not fully take into account certain cyber-operations that, by targeting other categories of data and without causing any second-order physically violent effect, would nonetheless cause serious consequences for the civilian population. This issue had been recognized by the ICRC, which in 2015 expressed ‘increasing concern about safeguarding essential civilian data’,[[255]](#footnote-255) claiming that:

‘[I]t would be important to clarify the extent to which civilian data […] such as social security data, tax records, bank accounts, companies’ client files or election lists or records, is already protected by the existing general rules on the conduct of hostilities. Deleting or tampering with such data could quickly bring government services and private businesses to a complete standstill and could cause more harm to civilians than destruction of physical objects. The conclusion that this type of operation would not be prohibited by IHL in today’s even more cyber-reliant world […] seems difficult to reconcile with the object and purpose of this body of norms.’[[256]](#footnote-256)

This statement was later echoed with almost identical words by the minority position within the group of experts that drafted the Tallinn Manual 2.0, who criticized the majority position as being under-inclusive:

‘[F]ailure to include cyber operations targeting data *per se* in the scope of the term ‘attack’ would mean that even the deletion of essential civilian datasets *such as social security data, tax records and bank accounts* would potentially escape the regulatory reach of the law of armed conflict, thereby running counter to the principle…that the civilian population enjoys general protection from the effects of hostilities. […] The key factor, based on the underlying object and purpose of Article 52 of Additional Protocol I, is one of severity of the operation’s consequences, not the nature of harm. Thus, they were of the view that, at a minimum, civilian data that is essential to the well-being of the civilian population is encompassed in the notion of civilian objects and protected as such.’[[257]](#footnote-257)

These concerns were shared by other authors.[[258]](#footnote-258) In particular, Cordula Droege argued that the functionality test ‘makes no sense’ in information technology, because ‘data can always be restored or changed there is no permanent and complete loss of functionality of an object short of physical damage’.[[259]](#footnote-259) Therefore, she argues that ‘an attack must also be understood to encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary.’[[260]](#footnote-260) In relation to this, it is worth noting how this approach has been recently endorsed by the French Ministry of Defense, in its 2019 document titled ‘Droit International Appliquè aux Opérations Dans le Cyberspace’ (‘International Law Applicable to Cyberspace Operations’).[[261]](#footnote-261) In France’s view, cyber operations may constitute attacks within the meaning of Art 49 AP I not only if they produce physical damage, but also if they render a system inoperative, that is, when the computer systems of the adversary no longer function as they were intended, whether temporarily or permanently, reversibly or not.[[262]](#footnote-262) The above mentioned statements are a strong signal of departure from the KEE test, echoing Noam Lubell’ s claim that ‘there is strong reason to question whether physical damage is the most appropriate threshold’, arguing that ‘the insistence of remaining focused on physical [damage to] property may require rethinking.’[[263]](#footnote-263) I believe that these critiques all correctly address the shortcomings of the KEE test, which become apparent when one tries it to apply it to the principles of distinction. Consider, again, that cyber-operations similar to those described above under Scenario 4 and 5 would be permissible under the KEE test. This would not only mean endangering the civilian population, but also creating a discrimination between member of the armed forces and civilians directly participating in hostilities. In fact, while the former category can be targeted by virtue of their status, civilians directly participating in hostilities can only be attacked for acts that, *inter alia*, reach a certain threshold of harm. Beyond acts adversely affecting the military capacity of the adversary (which would include also cyber-operations directed at military objectives, and not resulting in physical violence), the notion of harm is limited to acts causing physical violence to civilians and civilian objects. As a consequence of this, a civilian would be considered as taking a direct part in hostilities if he launches a cyber-operation that disrupts the enemy’s command and control network, as the cyber operation would adversely affect the military capacity of the adversary.[[264]](#footnote-264) However, if the same individual would launch a cyber-operation as those described under Scenarios 4 and 5, the individual would still be considered as a civilian since the effects of the cyber operations will not meet the threshold of intensity as interpreted under the KEE test. As a result of this, such individual could operate with impunity. Clearly, this is not an acceptable legal outcome.

### 2.2. Alternative approaches to the KEE Test.

#### 2.2.i. The notion of ‘military operation’ as the main condition for the applicability of the rules of targeting.

#### To overcome the interpretive questions posed by the KEE test, several alternative approaches have been proposed, which I will now examine. The most expansive view has been advanced by Niels Melzer, who argues that what is relevant for the application of the rules of distinction, proportionality and precaution is the concept of ‘military operation’ and not the notion of ‘attack’.[[265]](#footnote-265) Military operations are defined by Art. 48 and 51 of API as ‘all movement and acts related to hostilities that are undertaken by the armed forces’.[[266]](#footnote-266) Hence, even a cyber-operation which causes non-physicalviolent consequences and would not, under the Tallinn Manual interpretation, qualify as an attack, should nonetheless fall within the broader notion of military operations and subjected to the limits imposed by the law of targeting. While this interpretation aims at circumventing the interpretive problems associated with the definition of ‘attack’ in the cyber-context, it does not stand against a systematic reading of Part IV of API, which deals with the protection of civilians and civilian objects: as Roscini points out the ICRC commentary clarifies that section IV applies only to attacks, that is, to military operations during which violence is used.[[267]](#footnote-267) Furthermore, API operates a distinction between attacks and military operations with regards to the obligations that belligerents have to comply with in order to protect the civilian population and objects. In fact, while attacks are subjects to the principles of distinction, proportionality and precaution, military operations are merely subject to the more generic obligation to take constant care. This interpretation is therefore untenable.2.2. ii. The concepts of ‘capture, destruction and neutralization’ as qualifiers of an attack.

A different view has been put forward by Dormann, who argues that what qualifies an act as an ‘attack’ does not include mere destruction of objects, but also other modalities of interaction, namely capture and neutralization, as suggested by the definition of ‘military objective’ under Art 52 (2) of AP I.[[268]](#footnote-268) This approach has two main weaknesses. Firstly, it relies on the definition of military objective which, in turn, implies the existence of an attack in the first place, since its sole purpose is to determine if combatants can lawfully target an object or shall refrain from attacking it because it is not a military objective. Secondly, it focuses on the methods used to achieve a military advantage, namely destruction, capture and neutralization. However, while ‘destruction’ is closely connected to the causation of physical violence and can be interpreted extensively to include destruction of *digital data*,[[269]](#footnote-269) the same cannot be said with regards to the other methods. In fact, ‘capture’ refers to acts of ‘seizing and maintaining control or possession of an object’,[[270]](#footnote-270) while ‘neutralization’ can be described as ‘an attack for the purposes of denying the use of an object to an enemy *without necessarily destroying it*.’[[271]](#footnote-271) As we can see, since violence is not an essential elements of neither of the two concepts, they cannot be simply employed as qualifiers for what is an ‘attack’. Having said that, the approach taken by Dormann can be explained by considering that a cyber-operation might adversely affect the military capacity of the adversary even without causing physical damage or destruction to an object. It does not, however, clarify whether cyber-operations directed against civilian objects, and which do not result in second-order physical violent consequences, should be qualified as attacks or not.

## 3. Towards an Evolutionary interpretation of the notion of violence.

The above paragraphs have critically discussed the main doctrinal approaches to the notion of attack in the context of cyber-warfare, arguing that they all fall short, in one way or another, in providing an effective answer as to how to apply the definition of ‘attack’ to cyber-operations. It is submitted, in this regard, that the definition of attack in the cyber-context must be complemented with a reinterpretation of the concept of violence. Only in this way, then, it would be possible to provide effective protection to the many facets of human dignity that might be endangered by cyber-operations. The first step of this approach is to adopt an evolutionary interpretation to the notion of violence, whichis a method employed to clarify the meaning of terms within a treaty, and it is based on the assumption that the ordinary meaning of a certain term can evolve over time.[[272]](#footnote-272) The method was firstly qualified by the ICJ in the *Navigational Rights* judgment.[[273]](#footnote-273) The case revolved around a dispute between Costa Rica and Nicaragua in relation to the navigational and related rights of Costa Rica over the San Juan River, who sits on the border between the two States and on which Nicaragua has sovereignty. The contentious point involved the interpretation of Article VI of the 1858 Treaty on Limits between Costa Rica and Nicaragua, which gave the former a perpetual right of free navigation in relation to ‘objetos de comercio’.[[274]](#footnote-274) In this regard, Costa Rica claimed that it meant ‘for the purposes of commerce’, a term that included any activity or dealing between persons, including the transportation of passengers and the use of the San Juan river by Costa Rican officials providing public services.[[275]](#footnote-275) Conversely, Nicaragua favoured the more restrictive meaning of ‘with the articles of commerce’, which was limited to ‘the purchase and sale of merchandise, of physical goods, and excluded all services, such as passenger transport.’[[276]](#footnote-276) Furthermore, Nicaragua argued that, even if Article 6 was translated as to signify ‘for the purposes of commerce’, that would not have made any difference, since the term ‘commerce’ had to be interpreted according to the meaning it possessed when the Treaty was signed in 1858, at which time the term merely referred to trade in goods and excluded services.[[277]](#footnote-277)The Court disagreed with Nicaragua’s argument, holding that the term should have been interpreted in lights of its current meaning. That is because, in situations where the parties employed a generic term (such as ‘commerce’), they were aware that its meaning could evolve over time, and where the treaty has been entered into force for a very long time, it must be presumed, as a general rule, that the parties have intended the term to have an evolving meaning.[[278]](#footnote-278) While the *Navigations Rights* case proves its usefulness in explaining the operativity of the evolutionary interpretation principle, there are several judgments by international tribunals offering further examples of its application. For instance, in the *Gabcikovo-Nagymaros* case the ICJ considered that the terms of the bilateral agreement between Czechoslovakia and Hungary should be interpreted taking into consideration the law and scientific knowledge as they evolved at the time the case was decided before the Court and not at the time the treaty was concluded.[[279]](#footnote-279) A similar approach has been also endorsed by other international courts, such as the European Court of Human Rights, as well as the Inter-American Court of Human Rights, which have interpreted human rights treaties as ‘living instruments’.[[280]](#footnote-280) Evolutionary interpretation has also been employed within the *jus in bello* normative framework, where the landmark case is the ICJ‘s *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*. Faced with the question whether, absent any express treaty provision that banned the use of nuclear weapons, their use should have been considered lawful under IHL, the Court argued that the exclusion nuclear weapons for the application of the principles of IHL ‘would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of weapons, those of the past, those of the present and those of the future’.[[281]](#footnote-281) The reasoning of the ICJ, while related to the more general issue of the applicability of IHL to a certain weapon technology, is however an unquestionable example of how a specific term (in this case, ‘weapons’) was interpreted in an evolutionary manner. Similar considerations can be transposed to the cyber context, by interpreting the definition of attack under Art. 49 AP I in a way that takes into account the fact that cyber-attacks represent a kind of violence that differs from kinetic weapons in ways that were not conceived when the Additional Protocols were drafted. Considering cyber-violence as a new category is nothing new or innovative: after a UNGA resolution inviting Member States to submit to the Secretary General proposals in the field of information security,[[282]](#footnote-282) Panama argued that focusing only on kinetic effects of cyber-attacks was a flawed approach, since “computers today regulate many critical aspects of societies such as emergency services, air traffic, and financial information”, and therefore “an attack in which new information and telecommunication technologies are employed may cause more damage, for instance, than a conventional bombardment.”[[283]](#footnote-283) In this regard, the focal point is how exactly the notion of violence should be re interpreted.

### 3.1. The limits of reinterpreting ‘violence’ as including destruction of digital data.

One way to look at the issue is to re-envisage the concept of physical violence on a quantitative level, that is, to include cyber-operations resulting in destruction, alteration or disruption of digital data within the meaning of attack. This approach has been proposed by different authors,[[284]](#footnote-284) among which Heather Harrison Dinniss and Kubo Mačák. [[285]](#footnote-285) To this end, I will primarily critique Mačák’s approach, since it expressly relies on an evolutionary interpretation of the word ‘object’ which, in turn, leads to a wider understanding of the notion of violence. The case for interpreting data as ‘objects’ for the purposes of IHL begins, according to Mačák, by recognizing that the drafters of the ICRC conceived objects as something ‘tangible and visible’, in order to avoid that abstract concepts such as ‘civilian morale’ or ‘the aim or purpose of a military mission’ could be qualified as military objectives.[[286]](#footnote-286) However, Mačák claims that while *data,* unlike most objects, cannot be physically touched, they can nonetheless be seen and perceived by the human eye, and this trait alone is sufficient for qualifying *data* as something which is ‘visible’ and, ultimately, ontologically different from an abstract concept. Hence, it follows that the ICRC Commentary did not go as far as expressly excluding from the concept of objects immaterial entities, such as digital data, whose existence, considering the time in which the Protocols were ratified, could not even have been envisioned by the drafters of the Protocols.[[287]](#footnote-287) The legal consequence of this reasoning is that, since digital data can be interpreted as an ‘object’ for the purposes of the *jus in bello*, therefore any cyber-operation that causes damage or destruction of *digital data* would constitute violence, hence the cyber-operation that originated it would qualify as an attack.[[288]](#footnote-288) While I recognize that this interpretation has far-reaching, positive effects when it comes to determining what amounts to a ‘military objective’ in cyberspace, as we shall see in Chapter 4, I do not believe that destruction of digital data should be regarded as requirement to qualify a cyber-operation as an attack. To clarify my statement, let me consider the scenarios provided by Mačák to support his argument. Firstly, he points out that:

‘an attack [that aims to destroy data] may target critical data of a military nature, such as weapons logs, timetables for the deployment of military logistics or air traffic control information. Their destruction would not entail the use of physical force, yet it would fit the dual considerations of Article 52 (2). Such data makes an effective contribution to the military action of one party, in fact, its military action would be inextricably bound to ad based on this particular dataset. Its destruction would, therefore, also offer a definite military advantage to the opposing party.’[[289]](#footnote-289)

In this regard, I entirely agree with the consideration that data, being an object, might also constitute a military objective. Yet, it does not automatically follow that such a cyber-operation should be considered as an attack merely because data have been altered, interfered with, disrupted or destroyed. Rather, I believe that what makes the cyber-operation an attack is the military value of the target. This consideration is strengthened when we examine the second scenario presented by the author, where digital data of a civilian a nature are targeted, specifically ‘electronic health records held at a particular hospital.’[[290]](#footnote-290) Accordingly, Mačák notes that the cyber-operation would be qualified as an attack because ‘if this data were to be clandestinely erased or altered, the lives and health of patients in the hospital would be endangered’.[[291]](#footnote-291) In this situation, I believe that what makes the cyber-operation in question falling within the scope of Art. 49 is not just the destruction of civilian data, but the fact that its second order consequences might adversely affect values that needs to be protected by the *jus in bello*. This is something recognized by Mačák himself, as he points out how the destruction of data ‘would rather affect the integrity of the civilian object […] and the safety of the civilian population […].’[[292]](#footnote-292) To this end, one might even argue, as Michael Schmitt did, that the operation in question would constitute an attack also on the basis of the KEE itself, since it might result in injury or death to civilians, although it is questionable how this can be considered as ‘reasonably foreseeable consequential damage’, to use the words employed by Rule 30 of the Tallinn Manual 1.0.[[293]](#footnote-293)

The shortcomings of relying on data destruction as the essential qualifier of the notion of attack are more readily apparent if we recall that the concept of data is exceptionally wide, since it includes code that is essential for the functionality of computer system and networks, but encompasses also the surface content of websites, programs and personal files. It goes without saying that while every malicious cyber-operation involves, at some level, interference with digital data, not all of them entail adverse consequences. Consider for instance a website defacement which alters the graphical content of a website, a virus that corrupts the OS of a computer slowing it down or preventing it from booting correctly, or a cyber-operation that deletes email across different accounts. All these are examples of interference with digital data (content-level data and operational-level data) the consequences of which are not, in my opinion, serious enough to warrant any regulation by the *jus in bello*. Yet, if we assume that physical violence can include destruction or alteration of data, then all of the above instances, should they happen in the context of an armed conflict, would be qualified as attacks under Art. 49 AP I and would also trigger the application of the rules of targeting. This would mean, in practical terms, that if the perpetrator of the cyber operation is a civilian, they would be considered as directly participating in hostilities, and therefore be liable of being attacked. Clearly, I believe that reinterpreting the notion of physical violence to include destruction or alteration of digital data, without any additional qualifier as to what may or may not constitute an attack, creates the opposite issue that affected the KEE test: it is over inclusive and does not take into proper account the severity of the adverse consequences on the civilian population that may, or may not, arise from a cyber-operation. In conclusion, this interpretation leads to some problematic legal outcomes, would put too many uncertainties on the conduct of hostilities and would ultimately negatively impact the process of humanization. This does not mean that the interpretation of *digital data* as objects should be rejected in its entirety. On the contrary, it constitutes the basis of a new interpretation of the definition of ‘attack’ in the cyber context, which should go beyond the causation of physical violence as an essential requirement for the purposes of Art. 49 AP I and take in consideration different types of violence, as they are capable of severely affecting the dignity of the civilian population in its components of autonomy, liberty and wellbeing. More specifically, what I will be advocating for in the following sections is an interpretation of violence that extends to psychological violence and economic violence.

### 3.2. Psychological violence.

Psychological violence can be defined as the voluntary infliction of harm to the mental and emotional state of an individual.[[294]](#footnote-294) From a teleological perspective, considering psychological damage as ‘violence’ within the meaning of Art. 49 AP I is consistent with the overarching goal of protecting human dignity in armed conflict. In this regard, psychological violence affects the dignity of the individual by causing severe negative mental states such as fear, helplessness, and horror among others. Recalling that, as argued in Chapter 1, human dignity is a multi-layered concept, psychological violence can compromise the autonomy of the individual, by impairing their mental faculties and their ability to self-determinate; consequently, it diminishes their liberty in making appropriately informed decisions. In this regard, it is worth noting that the concept of psychological harm is, at least to some extent, already considered by the rules on targeting.More specifically, Art 51 (2) AP I prohibits acts or threats of violence aimed at spreading ‘terror’ among the civilian population, a provision that is engaged when terror ensues as a second-order consequence of an ‘attack’, that is, an act that already results in the causation of physical violence.[[295]](#footnote-295) In the context of cyberwarfare, the Tallinn Manual has adopted a similar approach, since it considers ‘terror cyber-attacks’ as falling within the prohibition under Art. 48 AP I, noting that:

‘While the notion of attack extends to injury and death caused to individuals, it is, considering the law of armed conflict humanitarian purposes, reasonable to extend the definition to serious illness and *severe mental suffering* that are tantamount to injury. […] Since terror is a psychological condition resulting in mental suffering, inclusion of such suffering in this Rule is supportable through analogy.’[[296]](#footnote-296)

The commentary to the Manual then goes on to explain that that a ‘cyber-attack against a mass transit system that causes death or injury’[[297]](#footnote-297) or ‘the threat to use a cyber-attack to disable a city’s water distribution system to contaminate water and cause death or illness’[[298]](#footnote-298) would qualify as an attack if it is launched with the intent to cause terror among the civilian population. Conversely, it is excluded that a tweet ‘falsely indicating that a highly contagious and deadly disease is spreading through the population’[[299]](#footnote-299) qualifies as a cyber-attack, as the Manual does not consider a tweet as an attack or a threat thereof. Leaving aside the likelihood that a similar kind of tweet can actually result in terror among the civilian population, it must be pointed out that the Manual’s approach is rather restrictive, since it considers terror as a qualifier of a cyber-attack only if it appears as a second-order consequence of an attack that causes physical violence. Beyond this, there is no meaningful contrast between the examples provided in the commentary. Thus, considering that the objective of the rules of targeting is to protect the civilian population from the harmful effects of attacks, there should not be any difference, from a legal standpoint, if psychological harm in the form of terror occurs as a second-order consequence of an act causing physical violence or not. This consideration is further reinforced by how the ICTY has interpreted the crime of torture under Art. 2 of the ICTY statute, which has been defined as ‘the voluntary infliction, by act or omission, of severe pain or suffering, whether physical or mental.’[[300]](#footnote-300) Furthermore, in the Limaj case judgment the Trial Chamber held that ‘there is not a requirement that the act or omission has caused a physical injury, as mental harm is the prevalent form of inflicting torture.’[[301]](#footnote-301) Having clarified that mental harm (that is, psychological violence) does not need to be caused by a previous act of physical violence to be regulated by jus in bello rules, the crux of the matter is what exactly amounts to ‘serious mental harm’.

In relation to this, the quantification of a of a *de minimis* threshold can be supported by analogy, by relying on the interpretation given by the ICTR to the notion of serious mental harm as one of the acts constituting the crime of genocide under the Stature of the ICTR.[[302]](#footnote-302) In Prosecutor v. Kayishema and Ruzindana, the Court, after reaffirming that ‘there is no prerequisite that mental suffering should be the result of physical harm’,[[303]](#footnote-303) argued that ‘serious mental harm’ should include ‘more than minor or temporary impairment of mental faculties’ further pointing out that ‘[…] the inflicting of strong fear or terror, intimidation or threat may amount to serious mental harm.’[[304]](#footnote-304) In a similar vein, the ICTY has noted that symptoms such as ‘temporary unhappiness, embarrassment or humiliation’, or a ‘mere state of anxiety’ would be ‘insufficient to establish serious mental harm.’ [[305]](#footnote-305) What needs to be proven, instead, is the causation of ‘grave and long-term disadvantage to a person’s ability to lead a normal and constructive life’.[[306]](#footnote-306) In this regard, I am certainly not comparing the mental suffering caused by torture or rape as a mean to commit genocide to that which can potentially result from certain cyber-operations. Rather, I am claiming that there might be certain cyber-operation that result in adverse effect on the mental state of the targeted individual which go way beyond irritation or inconvenience and may rise to the lower limit of serious mental harm, and the interpretive guidelines provided by the international criminal jurisprudence may constitute a useful tool for qualifying which of these operations amount to an attack and which do not. The kind of cyber-operations I am referring to are, for instance, operations of identity theft similar to the WannaCry and NotPetya ransomware attacks that affected hundreds of thousands of people worldwide between 2016 and 2017. The modus operandi of the crypto worms, as already mentioned in the Introduction, consisted in blocking access to the victim’s computer system and requesting the payment of a sum between 300 and 600 $ worth in Bitcoin. Furthermore, the cyber-attack targeted not only private individuals, but also companies like, most notably, the UK National Health Service (NHS). In such a situation there was no causation of physical violence, yet it has been shown that ransomware attacks cause irritability, fear, anger, significant anxiety and sleep deprivation,[[307]](#footnote-307) symptoms that could escalate into ‘severe distress and desperation, mistrust and paranoia’ in the medium to long-term. [[308]](#footnote-308) All these symptoms can be explained as the consequences of different factors, such as the exposure to potential financial losses, which are materialized in the form of a ransom to be paid. Moreover, there is the anxiety connected to the violation of the privacy of the victim, as it results from the encryption of the personal data. This anxiety is even magnified in the event of a ransomware that targets a hospital by the knowledge, by the affected individual, that their medical records are in the hands of malicious users.

Similar consideration can be drawn with regards to large scale episodes of identity theft directed against the civilian population. The scenario I am referring to revolves around the data breach which targeted the US Office of Personnel Management (OPM) in June 2015. The cyber-operation targeted personal records of 4 million employees, stealing 21.5 million of personal information records, including name, date of birth, home address, credit card details, social security numbers, tax file numbers, passport numbers, and digital fingerprint records.[[309]](#footnote-309) The cyber-operation can be classified as an act of cyber espionage, which the Tallinn Manual defines as ‘any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party.’[[310]](#footnote-310) In this regard, it should be noted that the hack merely exfiltrated personal records, rather than deleting or damaging them. In relation to this, Prof. Tim McCormack has argued that the hack should not be qualified as an attack, because data was not damaged in the process, and thus no ‘damage or destruction of objects’ actually took place; had the opposite happened, however, McCormack concedes that the operation should instead be considered within the meaning of Art. 49 AP I.[[311]](#footnote-311) This interpretation shows what, in my opinion, are the limits of a physically-focused definition of cyber-attack, whether it is the KEE test or the more evolutionary interpretation of data as ‘object’ which I believe McCormack is endorsing. What should count is not whether data have been destroyed or damaged, as I believe that compromising the integrity of data which was meant to be stored in a secured environment is functionally similar to destroying it. Rather, the determining factor is the relevance of the compromised data for the targeted individuals, and to what extent the data breach can affect their dignity to a sufficiently serious scale. Considering both the fact that a large number of individuals were affected by the cyber operation, as well as the personal nature of the records that were exfiltrated, I submit that the cyber-operation in question has certainly the potential of causing psychological violence to a significant degree and should be considered as an ‘attack’ if it is carried out in the context of an armed conflict. In conclusion, the notion of violence in the cyber context should be interpreted to include CNAs that cause psychological violence, provided that they met the sufficient threshold of severity of serious mental harm/serious psychological violence.

### 3.3. Cyber-operations causing economic violence.

The second category that is worth considering is economic violence, which can be defined as the forced deprivation of money, financial and material resources, or a combination thereof. The concept of economic violence is therefore very expansive, and ranges from theft to embargoes on selected categories of goods and services to other forms of economic sanctions. In the cyber context, economic violence can manifest itself as the second-order consequence of different categories of cyber operations. It can be, for instance, the direct consequence of a cyber-operation that steals valuable data or funds from the target system, as it has the case with the North Korean cyber-heist. In other cases, economic violence can be less straightforward and indirect, since it may result from the cost of repairing the functionality of the targeted systems, as well as from the economic losses suffered from the interruption of a certain service. As such, a cyber-attack like Shamoon caused economic violence both as a consequence of repairing the workstations (whose functionality had to be restored by purchasing brand new hard drives), and as a consequence of disrupting a service such as the oil distribution chain of Saudi Aramco. At this point, the essential question revolves around how, and to what extent, economic violence adversely affects human dignity. I believe that economic violence threatens human dignity by impairing the values of liberty and welfare. With regards to liberty, it essentially concerns the ability to act unrestrained by the will of others, in order to be able to act as a normative agent, that is, to autonomously decide over his own life. The capacity to exercise liberty can be threatened by physical violence and psychological violence, but can also be limited by economic violence, when the financial independence of the individual is diminished or compromised, for instance when their personal information are stolen or when the individual suffers monetary losses. Similarly, economic violence can adversely affect the ‘welfare’ element of human dignity, for instance by disrupting the provision of services which are important for the functioning of modern societies, such as the banking system, the provision of electricity, the production and distribution of commodities, public transportation and so on. Clearly, not every cyber operation that results in economic violence does affect the dignity of the civilian population to a significant degree, in a way that is should be considered as an attack. Rather, I believe that establishing a certain threshold of intensity is necessary: in this regard, I submit that only cyber-attacks causing serious economic violence should fall within the rubric of Art. 49 AP I. In order to determine when a cyber-attack reaches the required threshold of intensity, several factors can be examined on a case-by-case basis. For instance, the estimated economic losses suffered from the cyber-operation; the number of individuals it affected, and the extent to which it limited their liberty and wellbeing; how important was the function that was compromised or disrupted by the cyber operations, and so on. Clearly, they can appear cumulatively in one single instance or present themselves in isolation. In certain scenarios, finding serious economic violence can be done with relative ease. Consider again a case similar to scenario 4 in paragraph 1, in which a cyber-attack wipes the accounts of a bank; in a similar scenario, it would be safe to argue that every affected customer would have their liberty and wellbeing diminished. In this case, it can be identified a direct causal link between the economic deprivation suffered by individual, represented by the impossibility to use money, and the subsequent inability to fully provide for his needs: this, it is submitted, constitutes a violation of his dignity serious enough to be regulated by IHL. Similarly, the WannaCry/Petya ransomware attacks would also meet the threshold of serious economic violence had they happened during an armed conflict, both because they affected a large number of individuals and companies and because the services they affected were of great importance (targeted companies included the NHS and maritime shipping companies such as Maersk). There are other instances, however, where establishing the threshold of serious economic violence can be more problematic, such as in the case of the Shamoon cyber-attack, which not only affected the oil distribution chain of Saudi Aramco by erasing data from 30 thousands workstations but also caused an estimated economic damage of hundreds of millions of dollars. Should it be concluded that Shamoon qualifies as a cyber-attack? Leaving aside the question as to whether or not Saudi-Aramco could qualify as a military objective in an hypothetical armed conflict, if we merely look at the existence of a causal link between the damage caused by the cyber operation and a violation of dignity, it does not necessarily follow that it affected the economic resources of the targeted State to a point that the civilian population’s liberty and wellbeing was put at serious risk, mainly because the government of Saudi Arabia was able to restore the functionality of the affected workstations after ten days. However, one can ask what would have been the case if a similar cyber-attack was directed against a State with no financial and technical resources to limit the damage, or perhaps if the cyber-attack had targeted the oil production processes, instead of affecting just the way in which the oil was distributed. If such would have been the case, it could be reasonably argued that the civilian population’s wellbeing would have been affected on a much higher level and the operation would most likely be regarded as an attack. If anything, I believe that a cyber-operation like Shamoon, had it happened in the context of an armed conflict, should be regarded as an attack at least on the basis of their its potential to adversely affect the dignity of the civilian population on a serious level. In conclusion, while it can be argued that cyber-operations can have second-order consequences that amount to economic violence, it is submitted that only those reaching the threshold of intensity of ‘serious’ economic violence should be considered as cyber-attacks.

### 4. Conclusion: cyber-violence and the need for a taxonomy of cyber-attacks. The role of Critical National Infrastructures.

In light of the argument developed in the previous sections, it is possible to re-define the notion of cyber-attack in the following way: a cyber-attack is any cyber operation that is reasonably expected to cause physical violence, serious psychological violence, serious economic violence or a combination thereof. Is such an approach consistent with the goal of humanizing the law of cyber-targeting? On the one hand, an expansive interpretation of ‘attack’ will certainly broaden the protection of the civilian population and civilian objects against certain cyber-attacks that do not cause physical harm but can nonetheless violate human dignity on a significant scale. On the other hand, however, it would make the definition of attack subject to a greater degree of uncertainty.

The solution that has been suggested in this chapter is to adopt a requirement of intensity that would separate cyber-attacks causing mere inconvenience from those that would cause ‘serious’ consequences and would qualify as ‘attacks’ according to Art. 49 AP I. In the case of *physical violence*, the intensity criterion is satisfied whenever a cyber-attack is expected to cause death or injury to individuals and damage or destruction to objects. With regards to psychological and economic violence, the intensity criterion is more difficult to quantify. For this reason, it is submitted that the definition of cyber-attack must be supplemented by developing a taxonomy of cyber-operations that would be presumed to meet the required scale of intensity in relation to psychological and economic violence. In this regard, this Chapter has already provided examples of cyber-operations which would reach the ‘seriousness’ threshold, such as ransomware attacks, which cause psychological violence and economic violence to the target victim, and have therefore a negative impact on his dignity, as well as identity theft operations. Furthermore, another category worth including in this taxonomy are cyber-operations against Critical National Infrastructures (‘CNI’). Albeit there is no universal agreement on what exactly constitutes a CNI under international law, different states have defined the term in a similar manner. For instance, the *US Joint Terminology for Cyberspace* defines them as ‘systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such system and assets would have a debilitating impact on security, national economic security, national public health or safety, environment, or any combination of those matters, across any Federal, State, regional, territorial, or local jurisdiction.’[[312]](#footnote-312) The German definition is also similarly worded, since it includes ‘organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences’.[[313]](#footnote-313) The European Commission defines the notion of European Critical Infrastructure as ‘an asset or system or part thereof located in Member States which is essential for the maintenance of vital society functions, health, safety, security, economic or social well-being, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.’ [[314]](#footnote-314)These definitions of CNI, whether at State or regional level, share the common denominator that destruction or disruption of the functions of a CNI would affect several services which are connected to human dignity (especially the components of liberty and welfare) such as energy, food, water, transportation, banking, communication, financial and governmental sectors. [[315]](#footnote-315) The adverse effects stemming from the interruption or disruption of one of these essential services may vary, but their negative impact on the dignity of the civilian population must be presumed to be serious enough to qualify the cyber-operation that originated them as an attack. In certain cases, cyber-attacks against CNIs would cause consequences of a physical violent nature:therefore, they would fall under the application of Art. 49 or even more specific provisions of AP I related to prohibited attacks. For instance, a cyber-attack that targets the control system of a nuclear power plant causing a nuclear explosion and the release of massive spills of radioactive material would be considered as an attack under Art. 49, since it would cause massive physical violence in the surrounding area, both in terms of death or injury to individuals and damage and destruction of objects. Moreover, it would also violate the prohibition under Art. 57 to direct attack against installation containing dangerous forces, and may cause widespread, long-term and severe damage to the natural environment, thereby triggering the application of Art. 55. However, cyber-operations directed against a CNI and which do not result in physical violent consequences may nonetheless cause psychological or economic violence of a serious nature, and therefore should also be qualified as attacks – consider, again, a cyber-attack against the electrical power grid of a city or one that targets the banking sector of a State. Therefore, the definition of attack in the cyber context should be interpreted as including the following categories. Firstly, there are cyber-operations whose second-order consequences are likely to cause death, injury to civilians, destruction or damage to objects; these cyber-operations qualify as attacks because they cause physical violence. They would always meet the intensity threshold. The second category includes cyber-operations which would result in serious psychological violence and serious economic violence. Having said that, while this interpretation covers a broader list of cyber-operations than the KEE test, there are still certain categories of cyber-operations that would fall outside its scope of application. Certain cyber-operations will not reach the required threshold of intensity and would cause inconvenience to the civilian population: in this regard, website defacements, propaganda carried out through cyber means, DDoS attacks against governmental websites are all instances of cyber operation that do not fall under the meaning of Art. 49 AP I. In conclusion, if such an interpretation of cyber-attack would be adopted, it will be possible for combatants to determine, with a greater degree of certainty, what cyber activities are regulated by the law of targeting and, consequently, the possibility to minimize the adverse effect of such cyber-operations against the civilian population would be greatly increased.

# Chapter 3. The principle of distinction: civilians and combatants in the cyber domain.

In Chapter 1, I have argued that modern IHL is the result of the interaction between its two main driving forces, the principle of military necessity and the principle of humanity. On the one hand, the principle of military necessity stems from the assumption that violence is the constitutive element of any armed conflict, either international or non-international in character. Given the existence of a state of generalized and protracted armed violence, the principle of military necessity allows a belligerent to take all the measures which are ‘necessary for securing the end of the war’ and which are also lawful according to the *jus in bello.* On the other hand, the principle of humanity is based on the protection of human dignity, the core of which consists in autonomy- that is, the idea that every individual may exercise its normative agency to determine its own will without being constrained by the actions of others – and in its essential manifestations, liberty and wellbeing. In peace time, human dignity is protected through the conferral of a series of rights to the individual, encompassing the different facets of which autonomy is made, ranging from the protection of physical integrity to mental wellbeing, to the ability to make choices necessary for individual flourishing. In times of armed conflict, the protection of human dignity is enshrined in the principle of humanity, which acts as a limit to the principle of military necessity, both in the creation of the rules of IHL and in their interpretation. In this regard, Chapter 2 has demonstrated how the rise of cyberwarfare shakes the foundations of the modern *jus in bello*, by questioning the meaning of ‘violence’ within the notion of ‘attack’, which is the precondition for the applicability of the rules on targeting. After having proposed an expansive interpretation of what constitutes an ‘attack’ in the cyber domain, the objective of this chapter is to examine and discuss to what extent the principle of distinction applies to the cyber domain, and how it affects the relationship between human dignity and military necessity considerations. In order to do so, I will begin by examining the distinction between civilian and combatants. The principle is widely considered as one of the cornerstones of the law of targeting and represents the area of the *jus in bello* where the tension between the military necessity and the protection of human dignity is most evident. Thus, according to Art. 48 of Additional Protocol 1:

‘In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.’[[316]](#footnote-316)

As already discussed *supra* in Chapter 1, the *rationale* underlying the principle of distinctionis that there exists a military necessity to kill and capture combatants, and thus violate their dignity, because they are causally contributing to the existence of an armed conflict. At the same time the law rewards lawful combatants who ‘have fallen in the hands of a Party to the Conflict’ with the status of Prisoner of War (P.O.W.), from which certain rights and guarantees are derived, aimed at ensuring that captured combatants are nonetheless treated with humanity and that their dignity is respected.

On the other end of the spectrum lies the civilian, who does not engage in warfighting and, thus, does not represent a threat. Therefore, the *jus in bello* prohibits direct attacks against the civilian population, thereby ensuring that their dignity is protected. However, a civilian may lose its immunity from being attacked and become a lawful target as long and for such time as he takes a direct part in hostilities. Thus, combatant status and the notion of direct participation in hostilities (hereinafter ‘DPH’) are the two essential elements around which the relationship between military necessity and human dignity-driven considerations unravels. As such, the following Chapter will analyse how the two concepts are affected by cyberwarfare, beginning with an examination of combatant status in Section I, before discussing the notion of DPH in Section II. Section III provides a conclusion.

## 1. The Status of Combatant in Cyber Warfare.

The concept of *combatant status* is the essential to the principle of distinction. In the history of the *jus in bello*, lawful combatancy has been encouraged, even rewarded, with granting of Prisoner of War status to soldiers ‘falling in the hands of the detaining Power.’[[317]](#footnote-317) It is not the purpose of this section, however, to examine the set of rights of POW and the obligations incumbent upon the Detaining Power; rather, its focus is on the examination of the conditions of lawful combatancy and how they can be applied in the cyber context.

According to Art. 4 of the Third Geneva Convention, POW status is granted to the members of the armed forces to a Party to the conflict and members of military or volunteer corps incorporated in the armed forces. Members of the armed forces of a State are thus considered lawful combatants by virtue of their membership alone. The attribution of POW status applies also to members of the armed forces whose primary responsibility is to operate in the cyber context. As already evidenced in the Introduction, several States have already established cyber-units within the armed forces, such as the US CYBERCOM, the UK Joint Cyber Forces and the China’s People Liberation Army (PLA) Unit 61398. In addition, lawful combatancy is also granted to other militias groups, provided that they satisfy the four cumulative requirements of being under responsible command, having a fixed distinctive emblem recognizable at a distance, carrying arms openly and conducting their operations in accordance with the laws and customs of war. In addition to the four conditions explicitly mentioned by Art. 4, two more can be deduced from the text of the article: a certain level organization and the requirement of belonging to a party to the conflict.

1.1. Being under responsible command and being organized.

The first condition has been designed to discourage individuals from independently waging a war on the enemy instead of joining an organized armed group or the armed forces of a State. The *rationale* of the rule is that if a lone individual participating in an armed conflict without being commanded by someone responsible for his actions, it is very likely that such an individual would not comply with the rules of IHL. It is, in other words, a way to ‘keep rogue actors from the rubric of the war’.[[318]](#footnote-318) The condition is of straightforward application, both in the physical and in the virtual battlefield.[[319]](#footnote-319)

With regards to the organizational requirement, the way it has been construed by international criminal tribunals allows to take into account different degrees and types or organization. This is evidenced in *Akayesu*, where the ICTR found that a sufficient level of organization means ‘to enable the armed group or dissident armed conflict to plan and carry out concerted military operations, and to impose discipline in the name of a *de facto* authority.’[[320]](#footnote-320) Furthermore, in *Boskoski and Tarculovski*, the ICTY provided a list of factors that can be used to determine if the requirement has been satisfied. Firstly, whether the group has a command structure, which includes the establishment of a general staff or high command that appoints and gives directions to commanders, organizes the weapon supply, authorizes military action and authorizes individuals in the organization. Then, the Court included factors indicating that the group can carry out organized operations, like the ability to conduct large-scale military operations, or if the armed group controls any territory. Logistical capabilities have also been taken in consideration, like the ability to provide military training and recruit new members, as well as factors indicating that the group possesses a level of discipline and the ability to implement the obligations of CA3, such as the establishment of disciplinary rules and mechanisms. Lastly, the ICTY looked at the ability of the group to speak with one voice, a factor evidenced by the capacity to speak on behalf of its members in political negotiations. [[321]](#footnote-321)

In cyberspace, the element of virtuality adds a layer of complexity to the matter, as certain factors signalling organization, such as control over territory, the existence of headquarters or the supply and use of uniforms, have been designed to be applied to the physical battlefield and cannot be analogized to the cyber scenario, as they would be irrelevant. Considering this, it must be pointed out that, in principle, there is nothing that prevents a group of hackers from satisfying the requirement, even if the group is virtually organized and all its activities take place online; as such, the Tallinn Manual has correctly taken view that ‘failure of the members of the group physically to meet does not alone preclude it from having the required degree of organization,’[[322]](#footnote-322) as long as the group can show, as a minimum necessary element, to be under responsible command.[[323]](#footnote-323) However, the majority of hacktivists groups,[[324]](#footnote-324) such as Anonymous, or Cyberberkut, often resemble a collective of individuals, associating together by ideological reasons, but lacking a proper hierarchy or central authority. Understandably, it must be concluded that the mere fact that a group of individuals operates towards a collective goal, without possessing any element that might signal the existence even of a command structure, does not suffice to qualify the group as ‘organized’ for the purpose of granting combatant status to its members.[[325]](#footnote-325)

### 1.2. Requirements of distinction -Wearing a fixed distinctive emblem and carrying arms openly.

#### 1.2.i. Wearing a fixed distinctive emblem recognizable at a distance.

The rationale of the requirement is that of obliging combatants, in order to be entitled tolawfully participate in hostilities, to distinguish themselves from the civilian population. In this regard, Dinstein notes that its phraseology needs to be ‘reasonably construed.’[[326]](#footnote-326) This means that the assessment on whether a combatant is ‘wearing a fixed distinctive emblem’ is necessarily context specific. In situations of spatial and temporal proximity to the area where hostilities are taking place, it goes without saying that they must distinguish themselves from the civilian population by wearing uniforms recognizable at a distance. Conversely, there are instances in which the requirement is assessed more leniently: as such, combatants are not obliged to wear a fixed distinctive emblem when they operate in areas outside the combat zone or when they are off-duty.

In cyber warfare, where combatants are not in physical proximity of each other, analogous considerations apply.[[327]](#footnote-327) Consider, in this regard, a scenario where State A is in an international armed conflict against State B, and hostilities are taking place within the former State’s territory: suppose that a cyber-unit within State A’s armed forces, located some hundreds of kilometres away from the battlefield, launches a cyber-attack against a military compound where State B’s soldiers are present. Accordingly, the requirement of wearing an emblem recognizable at a distance does not extend to State A’s cyber unit, considering its practical inapplicability. Conversely, ‘where a combatant engages in a computer network attack in circumstances where they are in physical proximity to opposing forces [...], the requirement to wear a uniform or other distinctive mark would remain.’[[328]](#footnote-328)A more interesting question is whether the requirement of wearing a uniform or a distinctive emblem should be replaced with the obligation, incumbent on the attacker, that every cyber-attack should emanate from a designated IP address.[[329]](#footnote-329) Certainly, this would facilitate both compliance with the requirements and will also simplify the issue of attributing the cyber-attack to a specific State or armed group. However, this approach has also glaring weaknesses: as Heather Harrison Dinniss has fittingly argued, ‘requiring a computer to be marked as a military computer is tantamount to painting a bulls-eye on any system to which is connected.’[[330]](#footnote-330) To put it differently, since it would be much easier to identify the computer from which the cyber-attack has originated, as well all the computer networks and systems connected to it, they would be easily targetable – not only by the enemy, but from other ill-intended users as well. Secondly, further cyber-attacks emanating from the designated IP address would also be less effective, because secrecy is one of the essential elements for the success of any cyber-attacks. For these reasons, I do not believe that requiring that an attack emanates from a designated IP address would be an effective solution.

#### 1.2. ii. Carrying Arms Openly.

The requirement of carrying arms openly shares the same logic of ensuring that combatants must be distinguishable from the civilian population. In relation on how it applies to cyberwarfare, two specific issues are worthy of consideration. The first is of a preliminary nature and relates to whether cyber technologies can ever constitute a ‘weapon’ within the meaning of IHL. In this regard, the Tallinn Manual argues that cyber-weapons are ‘those cyber-means of warfare which are by design, use or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects.’[[331]](#footnote-331) The definition is closely connected to the notion of ‘attack’, which, as it has been examined in Chapter 2, has been interpreted by the Tallinn Manual as a synonym of physical violence. In the opinion of the present writer, this interpretation is too restrictive: rather, the notion of ‘weapon’ should be interpreted in accordance with the definition of attack that I have submitted in Chapter 2, whereby ‘cyber-attacks’ are those causing physical violence, serious psychological violence, serious economic violence, or a combination thereof. Applying this interpretation of attack to the notion of cyberweapon would lead to the conclusion that both malwares like Stuxnet (which caused physical violence) as well as Shamoon and CrashOverride/Industroyer (which caused serious economic violence and disrupted the provisions of certain services) would be considered as ‘cyberweapons’.

The second issue relates to the very relevance of the requirement of ‘carrying arms openly’ in the cyber context. According to the *Tallinn Manual,* it bears little significance in cyberspace, given its virtuality and the anonymity with which operators can launch cyber-attacks.[[332]](#footnote-332) While it is certainly true that the impact of the requirement is mitigated in the cyber context, there remain situations in which the requirement will still be relevant. For instance, certain CNA techniques, such as Internet Protocol (IP) spoofing, are carried out by concealing the identity of the attacker, so that the CNA appears to emanate from a civilian user domain. Therefore, it might be observed that conferring combatant status to individuals employing these methods ‘would violate the kernel of Article 4(2) (A) because it would risk civilian users being identified as the source/perpetrator of the attack’,[[333]](#footnote-333) thereby putting them at risk of being counter targeted. Such a legal outcome is unacceptable: therefore, it is submitted that the requirement to ‘carry arms openly’ should be interpreted to prohibit cyber-attach techniques in which the perpetrator of the cyber-attack conceals its identity and poses as a civilian user.

### 1.3. Belonging to a party to the Conflict.

The requirement of State affiliation demands that members of organized armed group must ‘belong to a Party’ to an international armed conflict. The main issue revolves around whether or not the requirement implies a high threshold, dependent on the law of State Responsibility, or whether a lower threshold is sufficient.

According to one view, a group ‘belongs to a Party to the conflict’ if its conduct is attributable to a State under Article 8 on the law of State Responsibility.[[334]](#footnote-334) In this regard, it is worth premising that there has been considerable disagreement between the ICJ and the ICTY in relation to what is the appropriate standard of attribution. In the Nicaragua case, the ICJ had to determine whether the acts of the *contras* in the territory of Nicaragua were attributable to the United States. The Court distinguished between two different scenarios. Firstly, it examined whether the *contras* could be acting as *de facto* organs of the United States, even if they lacked, *de jure*, the status of State Organs under U.S internal law. In this case, there must have been a relationship of ‘complete dependence’ between the *contras* and the United States.[[335]](#footnote-335) Having found there was no conclusive proof of such a relationship, the ICJ then moved on to consider whether the US could nonetheless be still held legally responsible. In this regard, the Court stated that for attributing the acts of the *contras* to the US there should have been evidence that the former exercised ‘effective control’ over the military operations of the latter. As such, even if the US were involved in financing, organizing, supplying and training the *contras*, this did not amount, according to the ICJ, to exercising effective control over ‘the military or paramilitary operations in the course of which the alleged violations were committed.’[[336]](#footnote-336) While the effective control test developed in Nicaragua has been endorsed by subsequent case law of the ICJ and by the International Law Commission, it has however been rejected by the ICTY. In *Tadic*, the Court had to classify the whether the armed conflict in the ex-FRY was international or non-international, for the purposes of determining the applicable law with which to try the defendant. In order to determine the nature of the conflict, the ICTY looked at whether the Army of the *Republika* *Seprska* (“VRS”), could be considered as ‘belonging to’ the Federal Republic of Yugoslavia within the meaning of Art 4 (A) (2) of the Third Geneva Convention. Had it been the case, the conflict between Serbia and Bosnia would have been qualified as international, therefore triggering the applicability of Art. 2 of the ICTY Statute. While in the Trial Chamber the Court relied on the effective control test to determine that the VRS did not belong to the FRY, the Appeals Chamber did not find the Nicaragua test persuasive or ‘consistent with the logic of the law of State responsibility’.[[337]](#footnote-337) What the Court did, instead, was elaborating its standard of attribution of ‘overall control’, which it deemed to be satisfied when a States has a role not only in the financing and equipping of an armed group, but also in coordinating or helping in the general planning of its military activity.[[338]](#footnote-338) Contrary to the *effective* control test, it is not necessary for a State to issue instructions to the group for the commission of specific acts contrary to international law. [[339]](#footnote-339) However, the suitability of the overall control test as a standard of attribution has been criticized in by the ICJ in the *Bosnian Genocide* case, where it argued that, while it ‘may very well be the case’ that the overall control test can be employed as a mean to determine whether an armed conflict is international, it nonetheless ‘stretches too far, almost to the breaking point, the connection which must exist between the conduct of a State’s organs and its international responsibility.’[[340]](#footnote-340) In the cyber context, the overall control test would be a much easier to satisfy that the effective control test, which, however, appears to be the appropriate standard under the law of State responsibility. Considering this, it must be pointed out that it would be very difficult to provide evidence that a State has directed and given instructions for the launch of a specific cyber-attack, in order to exercise effective control over an organized armed group.

A different approach holds that ‘belonging to a Party to the Conflict’ is a low-threshold requirement,[[341]](#footnote-341) which is satisfied when there is a ‘*de facto* relationship between the resistance organization and the party which is in a state of war, but the existence of this relationship is sufficient. It may find expression merely by tacit agreement, if the operations are such to indicate clearly for which side the affiliated organization is fighting.’[[342]](#footnote-342)

It is submitted that this interpretation is preferable, for several reasons. Firstly, as a matter of law, Katherine Del Mar correctly argues that ‘an examination of the rules of attribution […] does not lend support to the proposition that the actions of individuals classified as combatants under Art 4(A) (2) of the Third Geneva Convention are necessarilyattributable to a State.’[[343]](#footnote-343) In other words, the satisfaction of the requirement of ‘belonging’ does not depend on whether the action of an armed group can be attributed to a State according to the law of state responsibility, but is contingent on whether an armed conflict is international in character. In turn, the classification of the nature of an armed conflict does not necessarily rest on the law of State responsibility. This has been confirmed by the ICJ *dictum* in the Genocide Case, where the Court recognized that ‘[t]he degree and nature of a State’s involvement in an armed conflict in another State’s territory which is required for the conflict to be characterized as international, can be very well, and without logical inconsistency, differ from the degree and nature of the involvement required to give rise to that State’s responsibility for a specific act in the course of the conflict.’[[344]](#footnote-344) Therefore, it is perfectly possible for an armed group to ‘belong’ to a Party to the Conflict without giving rise to any issue of State Responsibility, since two different thresholds –that of having a *de facto* relationship with a Party to the conflict, and that of being under the effective control of a State- would be employed. In the cyber domain, this would be the case for groups of hacktivists such as the Syrian Electronic Army: assuming that the armed conflict in Syria qualifies as an IAC, they would be considered as having a *de facto* relationship with (and ‘belong to’) the Syrian Government by virtue of their ties with the Al-Assad Family,[[345]](#footnote-345) without the need to satisfy the requirements of the *effective control* test.

Furthermore, a requirement that hinges on the existence of a *de facto* relationship is substantially easier to satisfy than the effective control test and, therefore, would facilitate granting POW status to those groups of hacktivists who already fulfil the requirements or organization and compliance with IHL. Finally, a lower threshold for the requirement of State affiliation is consistent with the goal of increasing the protection of the dignity combatants in the cyber domain by granting them POW related rights. There is in fact no reason to deny POW status to individuals who have a *de facto* relationship of allegiance with a State party to a conflict and who also satisfy the other conditions of Art 4 (2) (A).

### 1.4. Compliance with IHL.

In relation to this requirement, it is essential to underline that the level of compliance to be assessed is that of the armed group as a whole, and not that of the individual. As such, an individual member of the armed group would lose its status as a POW if the activities of the group run contrary to IHL. In this regard, the primary example of conduct against IHL rules is directing attack against the civilian population and civilian objects, as it violates the principle of distinction. In the cyber-context, the notion of ‘attack’ must be interpreted in accordance to what I have argued *supra* in Chapter 2, and includes cyber-operations that cause physical violence in the form of death or injury to civilians, damage or destruction to objects, as well as serious psychological violence, economic violence or a combination thereof. Therefore, if a group of individuals launches a cyber-attack against a civilian target, such as the Critical National Infrastructure of a State which does not, in itself, meet the requirements for being qualified as a military objective within the meaning of Art. 52 (2) AP I,[[346]](#footnote-346) then its members would lose POW status upon capture.

### 1.5. Members of a *levee’ en masse.*

The category of the *levee en masse* is regulated by Art. 4 (A) (6) of the Third Geneva Convention, which grants combatant status to the population of non-occupied territories who, on the approach of the enemy, spontaneously take up arms to resist the invading forces. Differently from members of the State armed forces and organized armed groups, members of a *levee en masse* are dispensed from satisfying the requirements of responsible command, organization and belonging to a Party to the conflict, but they must nonetheless carry arms openly and conduct their operations in accordance with IHL. The *levee en masse* category is of problematic application in the cyber-context, since it poses several interpretive issues that must be addressed. The first relates to the condition that members of a levee en masse must be ‘inhabitants of a non-occupied territory.’ Given that cyberspace is a virtual and a-territorial dimension, no occupation can ever exist in cyberspace and, therefore, this raises the issue of whether the territorial element is necessary to trigger the existence of a levee en masse. The Tallinn Manual, recognizing that a levee en masse ‘did not contemplate military operations deep into the enemy territory’, considers that the requirement should be construed narrowly, that is, so as to include the situation where a civilian population engages in cyber-attacks to resist a physical invasion of enemy forces, whereas acts of resistance to cyber-attacks the effects of which are comparable to an invasion would be excluded.[[347]](#footnote-347) In the opinion of the present writer, there is no reason for such a restrictive interpretation of the category of levee en masse, especially considering that its aim is rewarding spontaneous acts of patriotism,[[348]](#footnote-348) and, secondly, that the interpretation of the provision must follow the rules of interpretation of the VCLT, this it is not confined to what the drafters of the Hague Conventions had in mind in 1899 but should, instead, take into account recent developments of modern warfare. Secondly, in relation to the requirement of carrying arms openly, the main issue is how to preserve the balance between the human-dignity oriented consideration to confer POW status to members of a levee en masse and the requirement to carry arms openly. In this regard, as noted already in Section 1.2., a good compromise is to consider the requirement of carrying arms openly satisfied ‘when cyber operations are not conducted by feigning protected, non-combatant status within the meaning of the prohibition of perfidy.’[[349]](#footnote-349)

Finally, it has been observed that the factual occurrence of a cyber-levee en masse is unlikely, given that presumably very few individuals among the civilian population of a given State would possess the capabilities to launch cyber-attacks against an invading state. This appears, according to one view, in stark contrast with the historical narrative of the *levee en masse*.[[350]](#footnote-350) However, this concern can be dispensed with the fact that the numerical element is an important but not essential factor for the existence of a *levee en masse*, with participation ranging from the hundreds of thousands of individuals, to a minimum of a dozen.[[351]](#footnote-351) In conclusion, despite the factual occurrence of a *cyber-levee en masse* appears unlikely, the category is still applicable to the cyber context.

### 1.6. The requirements of lawful combatancy under Additional Protocol I.

Finally, it is worth examining the requirements on lawful combatancy under Article 43 and Article 44 of Additional Protocol I. With regards to Art. 43, its first comma states as follows:

‘The armed forces of a Party to a conflict consist of organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government of an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict.’[[352]](#footnote-352)

Since Art. 43 AP I merely reaffirms several of the conditions necessary for lawful combatancy, [[353]](#footnote-353) it does not give rise to any specific issue when applied to the cyber context, as similar considerations to those examined in the previous paragraphs would apply. In relation to Art. 44 AP I, its most innovative parts are its third and fourth commas. Thus, Art. 44(3) relaxes the requirement of distinction, as the obligation arises only when a combatant is ‘engaged in an attack or in a military operation preparatory to an attack.’[[354]](#footnote-354) Interestingly, Art. 44 (3) does not require combatants to carry arms openly, except in situations where ‘owing to the nature of hostilities’ combatants cannot distinguish themselves from the civilian population. In similar scenarios, a combatant that falls into the power of an adverse Party shall still retain its status as a POW, provided that he carries arms openly ‘during each military engagement, and during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.’[[355]](#footnote-355) Furthermore, Art. 44(4) provides that if a combatant fails to comply with the above-mentioned requirements, he would forfeit his POW status, however he shall nevertheless be treated with the same level of protections to those granted to POWs.[[356]](#footnote-356)

As far as conventional warfare is concerned, Article 44 has been harshly criticized. By restricting the temporal framework in which the requirements of wearing a fixed distinctive emblem and carrying arms openly would apply, it makes the distinction between lawful combatants and irregular forces extremely unclear.[[357]](#footnote-357) Most worryingly, by providing equal treatment between POW and combatants who have failed to adhere to the requirements of distinction, it also incentivizes non-compliance by irregular forces. Therefore, the vast majority of States that have ratified Additional Protocol I (this excludes the United States, Israel and Russia) have made reservations to the effect that the scope of application of Art. 44 is only limited to situations of non-combat related movements in occupied territory.[[358]](#footnote-358) I believe that similar concerns can be shared with regards to the cyber context, where, in any case, the practical impact of the rule must be adapted to the peculiarities and limitations of cyberspace. More specifically, I believe that in situations where hostilities take place in spatial proximity with the enemy, the requirement to wear a fixed distinctive emblem to the greatest extent possible should be prioritized over that of carrying arms openly That is because the scope of the obligation to carry arms openly under Art. 44 (4) (a) and (b) was meant to apply to scenarios of guerrilla warfare taking place in occupied territory or in wars of national liberation;[[359]](#footnote-359) its purpose was to encourage combatants not to conceal their physical weapons in situations where they could not distinguish themselves from the civilian population. Yet, as I have discussed in the above paragraphs, the requirement of carrying arms openly has a much narrower scope of application as far as cyber-weapons are concerned, since their potential to cause violence is not connected to their physical appearance. In other words, by openly carrying an assault rifle during a military operation, a combatant is capable of distinguishing himself from the civilian population because he is unequivocally signalling that he is about to commit an act of violence against the enemy. A cyber weapon, instead, may be stored within computer system or in a USB driver, which are objects of everyday use and are not traditionally understood as being ‘signifiers’ of violence, at least not in the same way that kinetic weapons are. In conclusion, therefore, the only practical way to reconcile the logic of Art. 44 with the reality of cyberwarfare is that of interpreting the rule as requiring a cyber-combatants, in situations of guerrilla warfare happening in occupied territories or in wars of national liberation, to comply to the greatest possible extent to the obligation to carry a fixed distinctive emblem. Failure to do so would deprive the cyber-combatant of his POW status.

## 2. The notion of Direct Participation in Hostilities.

### 2.1. Historical Evolution of DPH. The distinction between civilian and combatant and the lack of a treaty-based definition.

While combatant status is regulated in detail in The Hague and Geneva Conventions, regrettably there is not a single rule of the *jus in bello* that specifies what are the essential elements of the notion of direct participation in hostilities (DPH) or, in other words, in what circumstances a civilian can be lawfully targeted. Rather, these components must be dissected from how the notion of *DPH* has been interpreted since its introduction in the 1977 Additional Protocols to the Geneva Conventions. As such, the resulting discrepancy between the concept of combatant status and DPH reflects how the rules on distinction have evolved over time and how the *jus in bello* has adapted to the changing character of modern conflict and the technological advancements in the means and methods of warfare.

Therefore, in order to understand how the notion of DPH applies in the cyber domain, it is necessary to briefly illustrate its historical evolution from the earlies days of the *jus in bello* to the present day. In this regard, we can see that the law of armed conflictof the late nineteenth centuryreflected a State-centric idea of warfare, which was regarded as ‘a political instrument at the disposal of a government, which held ultimate and exclusive authority over military force’.[[360]](#footnote-360) What followed from this conception is that war was considered ‘as the exclusive province of, and a state of affairs between, States.’[[361]](#footnote-361) This interpretation of the nature of war had far-reaching implications for the civilian-combatant divide. The civilian population was not only deemed of standing outside the battlefield but was also actively discouraged from participating in hostilities. According to Emily Crawford, this can be explained by the fact that civilians comprised ‘an unknown entity’ in war, certainly capable of fighting with fervour for the homeland but also lacking the skills and training that define professional soldiers. Consequently, the late nineteenth century *jus in bello* was ‘marginally concerned with civilian persons and their protection.’[[362]](#footnote-362) This is evidenced by two factors: firstly, civil wars and uprising were not regulated by any instrument, but were regarded as a matter of domestic law, which punished insurgents and militias as common criminals. Secondly, the law and did not define what elements made a combatant different from a civilian: rather, it identified the concept of combatant primarily with the figure of the professional soldier, to whom the law granted *combatant status*. In this regard, the law was keen to reward with the same status certain kinds of civilian participation in armed conflict, as shown by the 1899 Hague Convention Respecting the Laws and Customs of War on Land. In fact, Article 1 of the Convention extended its scope of application to militias and volunteer corps, provided they satisfied a set of cumulative requirements that professional soldiers were presumed to possess. As such, Article 1 of the Convention conferred the ‘rights and duties of war’ not only to armies, but also to militias and volunteer corps satisfying the four cumulative conditions of (i) being commanded by a person responsible for his subordinates; (ii) have a fixed distinctive emblem recognizable at a distance; (iii) carrying arms openly and (iv) conducting their operations in accordance with the laws and customs of war.[[363]](#footnote-363)

The Convention also dealt, to some extent, with resistance warfare, thus conferring combatant status to participants in a *levee en masse* under Art. 2. [[364]](#footnote-364)The article, however, did not apply to individuals participating in partisan warfare in occupied territories; instead, they were subjected to ‘principles of public conscience’ and ‘the laws of humanity’, as stated in the preamble of the Convention, known also as the ‘Martens Clause’.[[365]](#footnote-365)The subsequent 1907 Geneva Convention essentially reaffirmed the provisions of its predecessor, but implemented stricter conditions for granting the status of belligerents to participants in a *levee en masse*, adding the requirement to ‘carry arms openly’.[[366]](#footnote-366) In this regard, is it worth nothing that while The Hague and Geneva Conventions can be seen as an important step towards the extension of combatant status to civilians participating in hostilities between States, they lacked a definition of the essential elements of the notion of combatancy.

The trend persisted even after the adoption of the 1949 Geneva Conventions, which, beyond conferring new, humanity inspired rights to selected categories of individuals such as the wounded and sick and POWs, represented also a timely shift in paradigm, as they were the first instance where the *jus in bello* attempted to regulate civil wars and hostilities of a non-international character, as evidenced by Common Article 3.[[367]](#footnote-367)Yet, despite the article has been praised as being a ‘convention within the convention’,[[368]](#footnote-368) the Geneva Conventions did not resolve the issue of the legal status of civilians fighting in an armed conflict and not belonging to a *levee en masse* or to an organized armed group. The refrain from States in dealing with and regulating civilian participation in armed conflict is further reinforced by the fact that when the concept of direct participation in hostilities was firstly introduced by the 1977 Additional Protocols to the Geneva Conventions, it was, however, nowhere defined in their text. This normative vacuum that can be explained with the fact that States were not prepared to grant their own citizens’ the right to fight in an armed conflict’, as it ‘would […] undermine their claim to the monopoly of force, would promote the formation of non-state armed groups by those who are disenchanted, and encourage individuals to join such groups.’[[369]](#footnote-369)

Yet, since the first steps of the humanization process were laid down in the post-WWII era, warfare has faced profound transformations that made necessary to examine and clarify the fundamental elements of the concept of combatancy and, therefore, of the notion of DPH. The first shift occurred in the way wars have been fought: in fact, when Henry Durant arrived at Solferino in 1859, he witnessed the heinous effects of a battle that took place in a geographically limited area,[[370]](#footnote-370) where combat in close proximity was made a necessity by the technological limitations of the late nineteenth century. However, the Second Industrial revolution sparked dramatic innovations in the means and methods of warfare of the early twentieth century[[371]](#footnote-371). The perfection of artillery machines, the invention of new weapons such as machine guns and anti-personnel landmines, the development of submarines and, most notably, the employment of aerial warfare transformed the battlefield into the battlespace.[[372]](#footnote-372) This trend has shown no signs of interruption, and the advent of chemical and bacteriological weapons, Intercontinental Ballistic Missiles (ICBMs), Unmanned Aerial Vehicles (UAVs) and cyber weapons have had the effect of making belligerents unrestrained from spatial limitations and free to conduct hostilities ‘in a multidimensional battlefield, with weaponry the effects of which are felt much more on the civilian population than on combatants.

The second element impacting the rules on distinction is represented by the emergence of wars of national liberations, civil wars and, generally, non-international armed conflicts as the primary form of warfare in the post-WWII era, vastly outnumbering international armed conflicts.In these scenarios, civilians are far more likely to participate than in interstate wars and to outnumber soldiers in the number of casualties.

As a consequence of the interrelation of these trends, the role of the civilian in warfare evolved from that of being a spectator, estranged from hostilities, to that of playing an increasingly important part in the conduct of warfare. Civilians are now involved in many tasks, ranging from the manufacturing and maintenance of weapon systems, to the performance of security functions that have been outsourced from the military sector, causing the proliferation of Private Military Security Contractors (PMCs) in conflict zones like Iraq and Afghanistan. These factors have all contributed to blurring the distinction between civilians and combatants, and the development of cyberwarfare capabilities by State and non-State actors adds a further layer of complexity to the issue, as we shall see infra.

### 2.1. The interpretive attempts precedent to the ICRC’s Interpretive Guidance.

Therefore, given the lack of any treaty definition of the concept of DPH, the task has been taken on by military manuals, international courts and tribunals and the ICRC, in a process that involved multiple conceptual steps. In this regard, the ICRC Commentary to Additional Protocol I identified the kernel of the concept with the concept of harm, stating that ‘[T]he immunity afforded [to] individual civilians are subject to an overriding condition, namely, on their abstaining from any hostile acts. Hostile acts should be understood to be acts which by their nature and purpose are intended to cause actual harm to the personnel and equipment of the armed forces.’[[373]](#footnote-373)

States did not elaborate on the concept of harm but preferred, instead, to adopt a case-by-case approach, providing examples that would, or would not, constitute direct participation. Thus, the Commander’s Handbook on the Law of Naval Operations notes that ‘direct participation in hostilities must be judged on a case-by-case basis. […] Combatants in the field must make an honest determination as to whether a particular person is or is not taking a direct part in hostilities based on the person behaviour, location, attire, and other information available at the time.’[[374]](#footnote-374) The most recent edition of the US Law of War Manual reiterates that ‘whether an act by a civilian constitutes taking a direct part in hostilities is likely to depend highly on the context, such as the weapons systems or methods of warfare employed by the civilian side in the conflict.’[[375]](#footnote-375) Similarly, the UK law of war Manual also takes an analogous stance, stating that ‘whether civilians are taking a direct part in hostilities is a question of fact.’[[376]](#footnote-376)

By contrast, judicial bodies attempted to dissect DPH in detail, while still maintaining a case-by-case approach. The landmark case, in this regard, is the Targeted Killings judgment rendered by the Supreme Court of Israel.[[377]](#footnote-377) The case revolved around a claim brought via a petition by the Public Committee Against Torture in Israel (hereinafter ‘PCATI’) against the legality of the practice of ‘targeted killings’ undertaken by the state of Israel since the beginning of the second Intifada, aimed against ‘terrorists’ operating in Judea, Samaria and the Gaza Strip.[[378]](#footnote-378) According to the petitioners, targeted killings constituted a prohibited strike against civilians who, at the time they were targeted, were not taking a direct part in hostilities and were to be considered as a war crime. In this regard, the PCATI identified the essential element of the notion of DPH with the fact that a civilian is ‘openly bearing arms.’[[379]](#footnote-379) Conversely, the government of Israel argued in favour of a broader interpretation of the concept, which should have included persons who plan, launch, and commit attacks, even if such persons never actually use or carry the weapons utilized in the attack themselves.[[380]](#footnote-380) The Supreme Court of Israel attempted to balance the two approaches, recalling that ‘to restrict the concept to combat and active military operations would be too narrow, while extending it to the entire war effort would be too broad, as in modern warfare the whole population participates in the war effort, albeit indirectly.’[[381]](#footnote-381) Thus, when discussing whether transporting ammunition to the battlefield could be qualified as DPH, the Court observed that ‘[the] direct character of the part taken should not be narrowed merely to the person committing the physical act of attack, those who have sent him, as well, take a direct part. The same goes for the person who decided upon the act and the person who planned it’.[[382]](#footnote-382) Furthermore, the Court examined the meaning of the term ‘for such time as’, distinguishing between civilians committing sporadic acts of direct participation, who are only targetable for the duration of each specific instance of DPH, and individuals joining armed groups and committing a chain of hostile acts within that group, who could be targeted even between rest intervals between such acts.[[383]](#footnote-383) International tribunals further elaborated on the notion of direct participation, introducing the element of *belligerent nexus*. Thus, in *Strugar*, the ICTY held that to determine whether the conduct of a civilian constitutes DPH, regard must be had to ‘the individual circumstances of the victim at the time of the alleged offence.[[384]](#footnote-384) As the temporal scope of an individual’s participation in hostilities can be intermittent and discontinuous, whether a victim was actively participating in hostilities at the time of the offence depends on the *nexus* between the victim’s activities at the time of the offense and any acts of war which by their nature or purpose are intended to cause actual harm to the personnel or equipment of the adverse party.’[[385]](#footnote-385) The Court, regrettably, did not elaborate further on the notion of ‘nexus’.

Direct participation has also been examined by the ICC in several cases, the most impactful of which is *Lubanga*, where the Court dealt, *inter alia*, on the issue of direct participation by children. In this regard, it drew a distinction between ‘direct’ participation in hostilities, which relates to ‘combat participation’ and ‘active’ participation in hostilities, which covers combat-related activities such as ‘scouting, spying, sabotage and the use of children as decoys, courtiers or at military check-points.’[[386]](#footnote-386)

The major contribution to the notion of DPH came with the publication of the *Interpretive Guidance on the Notion of Direct Participation in Hostilities* by the ICRC in May 2009. The document, which has been the result of a three-year long process that involved both the ICRC and experts on the law of armed conflict, attempted to answer the question of who can be considered as a combatant under the law of armed conflict and, consequently, what are the main elements of the notion of DPH. The *Guidance* will, therefore, constitute the main basis upon which the relationship between civilian direct participation and cyber warfare will be examined.

### 2.2 The ICRC Guidance on Direct Participation in Hostilities: its constitutive elements and their application to cyber warfare.

According to the Guidance, the notion of direct participation in hostilities has a tripartite structure. Therefore, in order to qualify as DPH, an act must meet the following cumulative criteria:
‘(1) the acts must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or alternatively to inflict death, injury or destruction on persons or objects protected against direct attack (threshold of harm); (2) there must be a direct causal link between the act and the harm likely to result from that act, or from a coordinated military operation of which that acts constitutes an integral part (direct causation); and (3) the act must be specifically designed to directly caused the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus).’[[387]](#footnote-387)

#### 2.1.i. Threshold of Harm.The threshold of harm is satisfied when two alternative conditions are met. Either an act is ‘likely to adversely affect the military operations or military capacity of a party to an armed conflict’[[388]](#footnote-388) or is likely to ‘inflict death, injury or destruction on persons or objects protected against direct attack’[[389]](#footnote-389). As already discussed in Chapter 1, the requirement represents a compromise between military necessity and human dignity consideration, in that, as long as a civilian does not engage in harmful activities, there is no military necessity to kill or capture him. Conversely, if he performs militarily harmful acts or causes violence against the civilian population, then human dignity related consideration must yield against military necessity.

 a. Adversely affecting the military operations or military capacity of a party to an armed conflict.

The rationale of the first requirement is quite straightforward: provided that the elements of direct causation and belligerent nexus have been satisfied, a civilian loses his protected status and qualifies as a direct participant in hostilities when his activities can have a detrimental impact on the adversary military capacity or military operations. In this regard, the DPH specifies that ‘when an act may reasonably be expected to cause harm of a specific military nature, the threshold requirement will generally be satisfied regardless of quantitative gravity. Hence, it is pointed out that the requirement goes beyond the infliction of death, injury, or destruction on military personnel and objects, but includes any consequence adversely affecting the military operations or military capacity of a party to the conflict.[[390]](#footnote-390) In order to cause military harm an act must then adversely affect any activity that is ‘objectively useful in defence or attack in the military sense’[[391]](#footnote-391) or, in other words, any activity that relates to the war-fighting capacity of the enemy, such as acts of sabotage and other armed or unarmed activities restricting or disturbing deployments, logistics or communications, or capturing or otherwise exercising control over military personnel, objects and territory to the detriment of the adversary.[[392]](#footnote-392) *Vice versa*, acts that affect the enemy’s war-sustaining capacity do not cause military harm: for instance, acts of propaganda aimed at affecting the morale of the adverse party’s civilian population are clearly excluded. Lastly, the *Guidance* points out that failure to positively affect the military operations or military capacity of one of the parties to the conflict, such as the refusal of a civilian to collaborate as an informant, would not reach the required threshold of harm.[[393]](#footnote-393)

With regards to the cyber scenario, clearly a CNA that is intended to cause death or injury to soldiers or damage or destruction to military installations would certainly meet the threshold of harm; the same holds true for interference with military networks through cyber-means, an example that is recognized both by the *Guidance*[[394]](#footnote-394)and the *Tallinn Manual*. However, the *Guidance*’s approach can be criticized for being too restrictive, since ‘it focuses solely on the adverse effect on the enemy.’[[395]](#footnote-395) A preferable view has been adopted by the *Tallinn Manual*, which includes also ‘acts that enhance a part’s military operations or military capacity’[[396]](#footnote-396): the present author agrees with the above interpretation, since contributing to one side of the conflict usually means negatively affecting the military operations or capacity of the adversary. In that, harm and benefit are certainly two sides of the same coin, hence it would appear reasonable to adopt a lower standard when it comes to assess military harm, especially in the cyber-scenario. Therefore, activities like the maintenance of passive cyber-defence are also to be included within the threshold.

b. Inflicting death, injury or destruction on persons or objects protected against direct attack.

The second limb of the requirement includes acts that, while not adversely affecting the military operations or capacity of the adversary, are however likely to cause ‘at least death, injury, damage or destruction’ on persons or objects protected directed against attack, such as civilians and civilian objects. The requirement is modelled on the performance of ‘attacks’, defined by Art. 49 API as ‘acts of violence against the adversary, whether in offence or defence’[[397]](#footnote-397). Consequently, sniper attacks against civilians or the shelling of civilian villages are all acts that are likely to cause death, injury or destruction and would therefore meet the threshold of harm. Conversely, act that would not cause ‘violence’ within the meaning of Art. 49 AP I would not suffice for qualifying a civilian as directly participating in hostilities. Hence, the *Guidance* notes that activities like ‘the interruption of electricity, water, or food supplies’ and the ‘arrest and deportation of persons’, although they might negatively impact public security and health, would not met the required threshold of harm and, thus, would be excluded.[[398]](#footnote-398) In this regard, the second prong of the harm requirement has been construed in a very restrictive manner, and its application to the reality of cyber-warfare would lead to the exclusion of many cyber-operations directed against the civilian population, as they would cause no violence in the physical sense. Consider, for instance, the case of NotPetya, the worldwide ransomware attack that targeted primarily Ukrainian companies, banks and metro systems in June 2017, [[399]](#footnote-399)causing hundreds of millions of dollars in damage.[[400]](#footnote-400) If a cyber-attack of the scale of Not Petya occurs during an armed conflict, it would still fail to meet the required threshold of harm as it has been construed by the DPH Guidance. Such an outcome is legally problematic,[[401]](#footnote-401) as it allows the individual who has launched the cyber-attack to retain his protected status as a civilian and, ultimately, to operate with impunity. As already stated in this Chapter, I have argued in favour of a re-interpretation of the notion of violence that extends beyond the infliction of physical violence, in the form of injury, death, damage or destruction, to include also cyber-attacks that cause severe psychological and/or economic violence.[[402]](#footnote-402) Under this approach, the NotPetya CNA would satisfy the threshold, as well as other any other cyber-attack, that, despite not causing physical violence*,* can nonetheless produce adverse effect on human dignity, either by affecting the mental integrity of the civilian population or its economic wellbeing. There is, therefore, no reason to conclude that this kind of cyber-operations should be excluded from the range of acts the performance of which constitutes direct participation in hostilities: rather, I believe that a more expansive interpretation of the concept of violence would have the positive effect of widening the scope of application of the notion of DPH, discourage civilians from taking a direct part in hostilities and, ultimately, reinforce the application of the principle of distinction between civilians and combatants.

#### 2.1. ii. Direct Causation.

The second element of the notion of DPH requires the existence of a ‘direct causal link between a specific act and the harm likely to result either from the act, or from a coordinated military operation of which that act constitutes an integral part.’[[403]](#footnote-403)

Direct causation has been elaborated by the ICRC to relate the concepts of ‘direct’ and ‘indirect’ participation in hostilities to, respectively, the conduct of hostilities and war-sustaining activities, both of which ‘may ultimately result in harm reaching the threshold required for a qualification as direct participation in hostilities.’[[404]](#footnote-404) According to the Guidance, the difference is that while the former is designed to cause the harm, the latter merely maintains of builds up the capacity to cause such harm and is, therefore, to be excluded. In this regard, the essential element that satisfies the threshold of direct causation is the fact that the harm caused by an act ‘must be brought about in one causal step’.

The requirement has been construed rather narrowly: in fact, the commentary to the Guidance points out that is not necessary nor sufficient for an act to be indispensable to the causation of the harm, or to be connected with its consequences through an interrupted causal chain of events.[[405]](#footnote-405) Furthermore, the Guidance requires causal proximity between the act and the harm, as opposed to temporal or geographical proximity, as they bear no weight for the satisfaction of the threshold. [[406]](#footnote-406)

In this regard, it is necessary to point out that the approach of the Guidance appears unclear in several aspects, and has been criticized by different authors as being ‘under inclusive’, [[407]](#footnote-407) leading to uncertainty,[[408]](#footnote-408) and unsupported by treaty law and case law.[[409]](#footnote-409) In fact, the requirement of direct causation is not clarified by the ICRC, which merely enumerates a set of activities that meet the threshold because, presumably, they bring about the harm in a single causal step. Under this approach, several activities fall below the threshold, some of which are certainly too removed from the harm to meet the threshold of direct causation, such as the manufacturing of weapons. In other cases, however, the direct causation test appears to be unreasonably strict, as it leads to the exclusion of acts such as the assembly and storing of Improvised Explosive Devices (IEDs), which most States and legal scholars consider a clear example of direct participation.[[410]](#footnote-410) Yet, the requirement is assessed much more leniently in the context of collective operations, since it includes ‘conduct that causes harm only in conjunction with other acts’[[411]](#footnote-411), for which is sufficient that the hostile act is ‘an integral part of a concrete and coordinated tactical operation that directly causes […] harm.’[[412]](#footnote-412) Consequently, identification and marking of targets and intelligence gathering would met the direct causation standard despite the harm caused, which in this case would be of a military nature, would be several causal steps removed from the act.

When applied to the complex reality of cyber-warfare, the direct causation test yields similarly problematic results. There is, first and foremost, a problem of consistency in the assessment of certain categories of cyber activities: consider, for instance, the status of those who design and implement malicious code directed against a military objective or intended to cause harm to the civilian population. Given that the harm resulting from the cyber-attack would be too remote from the design and implementation of the code, such an activity would not meet the threshold. However, the same activity would satisfy the direct causation test if undertaken in the context of a coordinated military operation. Analogous considerations apply to those individuals involved in maintenance and support of computer networks for passive cyber defence, which would be excluded under the *Guidance’s* approach. Conversely, the Tallinn Manual consider considers this category of cyber-operations as satisfying the threshold of harm requirement.[[413]](#footnote-413) In relation to this, it is necessary to distinguish between immediate maintenance and support not of a routinary nature, which could qualify as direct participation, and ‘other routine maintenance’ which falls into a different category and should not be considered.[[414]](#footnote-414) It is the opinion of the present author that the *Tallinn Manual*’s approach is preferable:

Secondly, given that the requirement is limited to a single causal step between the act and the harm, this would exclude every single cyber-attack from ever meeting the direct causation test. In fact, as discussed in Chapter 2, cyber-attacks cause their effects in multiple causal steps: a CNA interacts with the digital data stored in a computer network or system, then it produces second-order and even third-order effects in the physical world, either in the form of physical violence, or by causing serious psychological and/or economic violence. In the cyber context, in other words, the harm is at least one causal step removed from the act, thus falling short from ever satisfying the threshold, unless the cyber-attack in question is part of a ‘coordinate military operation’. But even then, many cyber-attacks would not constitute conduct amounting to DPH.

To further illustrate why the approach of the *Guidance* is unfit for the cyber-context, it is useful to discuss how it applies to Stuxnet, had it happened in the course of an armed conflict. As already mentioned, the Stuxnet worm was launched in October 2009 against the uranium-enrichment site at Natanz, Iran. The code was specifically designed to target the Siemens Step7 software constituting the Supervisory Control and Data Acquisition System (SCADA) of the turbines operating within the facility, altering their rotatory speed while, at the same time, faking industrial process control sensor signals to prevent the infected system from shutting down from detected abnormal behaviour.[[415]](#footnote-415) As a result, it has been reported that the worm caused the physical degradation of more than a thousand machines over a two-year period.[[416]](#footnote-416) It is clear from the above that Stuxnet meets the threshold of harm as it caused a considerable amount of physical damage. However, it is also evident that the harm has been the result of a complex chain of events that begun with the infection of the target software by malicious code and ended with the actual physical damage of the turbines. As such, despite the harm unfolded through an interrupted causal chain, it would fail the direct causation test.

In light of these considerations, the direct causation requirement seems the hardest to satisfy in the cyber operations context.[[417]](#footnote-417)Understandably, such a conclusion bears troublesome consequences for the relationship between human dignity and military necessity, since it would allow many individuals to conduct harmful cyber-attacks, with no risk of losing civilian status, while, at the same time, it would forbid belligerents from targeting those very individuals, despite the military necessity to do so.[[418]](#footnote-418) In the cyber context, it is submitted that a better approach is to consider the threshold of harm satisfied even when the harm is connected with the cyber-attack through an interrupted causal chain of correlated events.

#### 2.1.iii. Belligerent nexus.

According to the *Guidance*, the requirement of belligerent nexus is satisfied when an act is specifically designed to directly cause the required threshold of harm in support to a party to the conflict and in detriment of another.[[419]](#footnote-419) The *rationale* of the principle is aimed at avoiding acts causing military harm or violence which are not connected with the hostilities, such as criminal violence or civil unrest aimed at expressing dissatisfaction with the territorial or detaining authorities,[[420]](#footnote-420) from being considered examples of direct participation. The *Guidance* also notes that belligerent nexus must be distinguished from subjective intent, which relates to the state of mind of the individual and not to the ‘objective purpose of the act.’[[421]](#footnote-421) In the context of cyber warfare, the determination of the belligerent nexus requirement does not pose significant interpretive issues. Certain activities would satisfy the requirement as long as they have a relation with the conduct of hostilities, like a cyber-attack launched by a group of patriotic hackers. Conversely, acts performed by ‘hacktivists’ such as Anonymous, who are moved by free speech concerns, fall short of meeting the threshold. A peculiar example of how the belligerent nexus relates to the cyber context is that of a DDOS campaign, where multiple categories of individuals are involved in different stages of this particular kind of cyber-attack: those who designed the code, those who executed the program and the unaware owners of ‘Botnets’, a terms used to indicate a network of infected ‘zombie’ computers used to flood designated internet addresses. How do these categories of individuals qualify, for the purpose of determining the existence of a belligerent nexus? In this regard, those who designed the code may or may not be considered as participating in hostilities. If the code was specifically designed to be used against the target State, then the requirement is easily satisfied; conversely, if those individual designed malicious code and then made it available through the internet it is reasonable to argue that there is no intent to cause harm to aid a party to a conflict and in detriment of another. In relation to the individuals who executed the code, the act of materially executing the cyber-attack certainly satisfies the threshold. Finally, the owners of infected ‘zombie’ PCs would be still considered as civilians,[[422]](#footnote-422) as the *Guidance* correctly excludes the existence of a belligerent nexus when civilians are either ‘deprived of their physical freedom of action’ or, as in this scenario, ‘unaware of the role they are playing in the conduct of hostilities’.[[423]](#footnote-423)

#### 2.1. iv. The temporal scope of Direct Participation in Hostilities.

Once an act cumulatively satisfies the requirements of threshold of harm, direct causation and belligerent nexus, the individual who has performed the act loses his status and can be targeted for such time as he directly participates in hostilities. The temporal element includes, first and foremost, the measures preparatory to the execution of an act constituting DPH; according to the *Guidance*, they correspond to ‘military operation[s] preparatory to an attack’,[[424]](#footnote-424) since are aimed to carry out a specific hostile act, as opposed to those measures ‘aiming to establish the general capacity to carry out unspecified hostile acts’,[[425]](#footnote-425) which do not make a civilian liable of being targeted. Moreover, the temporal element of DPH extends also to deployment and return from the location of the execution of the act.[[426]](#footnote-426) As far as the ‘physical’ battlefield is concerned, this approach represents a reasonably successful attempt at striking a balance between military necessity and humanitarian considerations.[[427]](#footnote-427)In fact, by allowing the targeting of an individual from the moment it engages in preparatory measures, belligerents ‘will have a reasonable window of opportunity to identify the threat and react to it before the hostile act is launched.[[428]](#footnote-428) In the cyber context, however, things are more complex. There are certainly situations where the temporal element of DPH can be ‘cyberized’ with sufficient clarity: for instance, the design of malicious code or the creation of Botnets, do not constitute ‘preparatory acts’ and do not entail loss of civilian status *per se*, unless they are aimed at executing a specific hostile cyber-operation.

For the most part, however, determining the time frame in which a civilian that is directly participating in cyber-hostilities can be targeted is difficult to pinpoint, since in cyberspace the preparation and execution of an act is carried out through multiple causal steps, each of which may be performed in a split-second, such as the acquisition of a target or the placement of malicious code within the target system. Therefore, as argued by Buchan, ‘by restricting direct targeting to only that specific timeframe when […] measures are undertaken, opposing forces will have a narrow window of opportunity to target the individual representing the threat.’[[429]](#footnote-429) In this regard, I believe that the optimal solution has been suggested by the Tallinn Manual, according to which the temporal element of DPH should commence ‘from the beginning of his involvement in mission planning to the point he or she terminates an active role in the operation.’ [[430]](#footnote-430) This approach properly addresses some potential issues which are peculiar to the cyber context, such as when a cyber-attack results in delayed effects, or effects that take place over time. Consider, for instance, a Stuxnet-like scenario in which an attacker places a ‘logic bomb’ in the target system in order to cause physical damage over a prolonged period of time. In this regard, the notion of ‘logic bomb’ describes a malicious code that, once inserted in a software, will activate itself at a future point, either on command, upon lapse of a certain period, or once the target system performs a specific action. In this scenario, the temporal timeframe for targetability would commence from the moment in which the attacker gains access to the target systems and extends for such time as the attacker has manual control of the malware; clearly, this also means that if the malware is a self-executing worm that does not need any external human intervention once it is activated, then the attacker’s direct participation should end once the malware’s payload is deployed. What is essential to underline, for the purposes of the present argument, is that the actual causation of the harm may happen when the timeframe in which the attacker may be considered as directly participating in hostilities has already elapsed. This approach, it is submitted, properly balances human dignity considerations with military necessity, as the temporal scope of targetability lasts as long as the individual involved in the cyber-attack is posing a threat to the opposing forces, and, therefore, as long as there is a military necessity to target him.

A contentious point relates to the loss of protection from direct attacks of hackers who commit repeated acts of direct participation over a determined period of time. The issue has already been approached by the DPH Guidance in the context of conventional warfare. Thus, according to the ICRC, ‘civilians lose protection against direct attack for the duration of each specific act amounting to direct participation in hostilities’.[[431]](#footnote-431) This differentiates them from members of organized armed forces belonging to a non-State party to an armed conflict, who can instead be targeted for as long as they assume a continuous combat function.[[432]](#footnote-432) In other words, ‘civilians lose and regain protection against direct attack in parallel with the intervals of their engagement in direct participation in hostilities’, which creates a ‘revolving door’ in which individuals may shift between civilian status and direct participation in hostilities. [[433]](#footnote-433) The concept of ‘revolving door’, which has been heavily criticized by the doctrine,[[434]](#footnote-434) has been defended by the ICRC as being an integral part of IHL, because its logic is aimed at preventing attacks on individuals who, at the time, do not represent a military threat.’[[435]](#footnote-435) I do not believe that this approach can effectively applied to cyberspace, as it would lead to the absurd result of requiring belligerents to target a civilian hacker ‘during each split second that a new cyber-attack is prepared, launched and conduced’,[[436]](#footnote-436) and ultimately preventing parties to the conflict ‘from pursuing their legitimate security needs.’ [[437]](#footnote-437) A better alternative, it is suggested, is to interpret the words ‘for such time’ as encompassing the entire timeframe during which the individual is engaged in repeated cyber operations. [[438]](#footnote-438) This timeframe begins with the first act of cyber-participation until the last and includes the intervals of rest or preparation between each cyber-attack, as there would be the military necessity to target the not only during the execution of these acts, but also between them.

## 3. Conclusion.

This Chapter has analysed the application of the principle of distinction to the cyber context and discussed how the need to protect human dignity can be balanced with military necessity considerations. In this regard, Section I has discussed the implications of combatant status in cyberwarfare, noticing that certain elements necessary for the granting of POW Status will be difficult to satisfy in the cyber context, such as the requirement of wearing a fixed distinctive emblem and that of carrying arms openly. Other requirements, instead, can be adapted to cyberspace without raising unsurmountable legal issues, such as those of organization, belonging to a Party to the conflict, and being in compliance with IHL. These are the requirements, in my opinion, that should be prioritized when determining whether or not a cyber-combatant should be granted POW status.

Section II has outlined that cyberwarfare presents peculiar legal issues in relation to the notion of direct participation in hostilities, especially with regards to how the component of ‘harm’ should be interpreted. In this regard, I anchored my interpretation of the notion of ‘harm’ to the definition of cyber-attack that I have elaborated in Chapter 2: that is, harm does encompass all cyber-operations that either adversely affect the military capacity of the adversary, or cyber-operations that result in physical violence, serious psychological violence, serious economic violence, or a combination thereof. Secondly, I have examined the temporal dimension of the concept of DPH, in relation to which I have argued that it must be interpreted in a way that allows combatants a reasonable amount of time to target the individual who is taking a direct part in cyber-hostilities, especially with regards to a situation of repeated instances of direct participation over a fixed amount of time. At the same time, especially in relation to cyber-attacks that have delayed or persistent effects, the temporal scope of DPH should be focused on the timeframe in which the hacker exercises control over the cyber-attack, and not necessarily on the moment in time in which the harmful effects manifest themselves. All things considered, I believe that the scope of application of the notion of DPH in cyberspace is significantly broadened. This consideration, on the one hand, may signify that individual hackers should be aware of the consequences of unlawfully participating in hostilities, and should be discouraged from doing so. On the other hand, a more expansive meaning of DPH also increases the potential number of individuals who may lose their protection against direct attack and can be targeted, by kinetic and/or cyber means.

# Chapter 4. The distinction between civilian objects and military objectives in the cyber domain.

As stated in Chapter 3, the *rationale* of the distinction between combatants and civilians is to balance the principle of military necessity with the need to protect the dignity of the civilian population. This objective is achieved by prohibiting not only on attacks against the civilian population, but also against civilian objects, thus requiring combatants to target only military objectives. Thus, according to Art 52 (2) AP I:

‘Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture and neutralization offers a definite military advantage.’[[439]](#footnote-439)

 The basic rule is then complemented by provisions related to the general protection of civilian objects; the protection of objects indispensable to the survival of the civilian population;[[440]](#footnote-440)the protection of the natural environment;[[441]](#footnote-441)and the protection of works and installations containing dangerous forces.[[442]](#footnote-442) Besides the two Additional Protocols, there are more specific rules found in different IHL conventions which are related to the protection of the natural environment[[443]](#footnote-443) and the protection of cultural property among others,[[444]](#footnote-444) all of which share the same *telos* with the general principle, that of protecting the dignity of the civilian population. That is because, as demonstrated in Chapter 1, human dignity extends beyond the physical integrity of the individual and encompasses all the physical spaces in which its liberty can be fulfilled and its wellbeing can be enjoyed, such as houses, schools, hospital or places of worship or any object that serves a civilian function. On the other hand, the only lawful target of attacks are military objectives because, unlike civilian object, ‘make a direct contribution to military action’ and ‘their destruction, capture or neutralization […] offers a definite military advantage’.[[445]](#footnote-445) Thus, the purpose of the following Chapter is to explore how the definition of military objectives applies to the cyber domain, to what extent if affects the balance between military necessity and humanity, and what does it mean to adopt an interpretation of military objective in the cyber context that aims at maximizing the protection of the civilian population.

1. The definition military objectives in cyberspace: the requirement of ‘objectness’.

Before doing so, however, it must be pointed out that only ‘objects’ may qualify as military objectives. As recalled in Chapter 2, the question of whether digital data can qualify as objects is far from settled, with the majority position within the Tallinn Manual arguing that data are not objects,[[446]](#footnote-446) and several scholars, including myself, aligning themselves on the opposite side of the interpretive spectrum.[[447]](#footnote-447) I believe that the reason why data should be classified as objects is, to put it simply, because it maximises the protection afforded to the civilian population by requiring combatants to comply with the principle of distinction and the rules of targeting. In practice, this means that combatants would be required, when they launch a cyber-operation, to determine whether or not the data they are targeting (for instance, the SCADA system of a power plant) can be considered as a civilian object or, rather, if it can be qualified as a military objective. If they determine the data to be civilian in nature, such data would enjoy protection from ‘attacks’ which, as discussed in Chapter 2, would include any cyber-operation that results in physical violence, serious psychological violence or serious economic violence, as I have discussed in Chapter 2. If, instead, the data in question qualifies as a military objective, combatants can lawfully target it, provided that the operation in question does not violate the principles of proportionality and precaution.In this regard, Heather Harrison Dinniss has rightly observed how excluding data from the notion of ‘object’ would lead to ‘manifestly unreasonable results’ when it comes to the applicability of the principle of distinction. As she has argued:

‘To take a practical example, weapons, weapons systems and military materiel are perhaps the epitome of a legitimate military objective. Examples include Stuxnet-type code, which is intended to cause physical destruction, or even viruses such as Wiper, which destroyed the functionality of computer systems without destroying any physical components. However, by excluding intangible objects such as code from the interpretation of the definition offered by the majority of the Tallinn group, neither of these cyber weapons would constitute a legitimate military objective. It cannot be correct that one can have a weapon that is made entirely from code that does not constitute a military objective.’[[448]](#footnote-448)

This statement has been the object of a rebuttal by Michael Schmitt, who notes that is irrelevant whether one considers a cyber-weapon made of code an ‘object’ or not:

‘If it falls within the meaning of 'object' […] the code accordingly qualifies as a military objective that may be lawfully attacked. If it is not an object […], the Article 52(1) prohibition on attacking civilian objects does not apply and the code may be targeted even if the operation results in destruction or damage to the code.’[[449]](#footnote-449)

That is because the Tallinn Manual’s interpretation on the term object applies only:

‘to determine when an object qualifies as a civilian object protected from attack pursuant to Art 52 (1), not to assess whether data qualifies as a military objective subject to attack […] The fact that an entity is not an object does not mean that it cannot be ‘targeted’. On the contrary, it means that the prohibition on attacking civilian objects does not apply. There is no need to determine whether the target is a military objective.’ [[450]](#footnote-450)

I think that Schmitt’s argument is not entirely convincing. That is because the notion of ‘object’ is the necessary prerequisite to determine when an object is a civilian or, if it meets the criteria specified by Art 52 (2) API, a military objective. This, of course, does not mean that the source code of Stuxnet, to use the example provided by Dinnis, cannot be ‘targeted’. But this term should be understood in its operational-tactical terms, not in a legal sense. To put it differently, a cyber-operation aimed at destroying Stuxnet’s source code would fall in a legal vacuum. That is because if we exclude, *a priori*, that digital data can ever be qualified as an object, this means that belligerents will not be required to determine whether or not the code of Stuxnet makes an effective contribution to military action, and whether its destruction, capture or neutralization would offer a definite military advantage. If data is not an object, it cannot be a military objective within the meaning of Art 52 (2), therefore the whole appraisal process would be pointless. Furthermore, the principle of proportionality would be inapplicable, too, because the so-called ‘proportionality equation’ rests on a comparison between the military advantage anticipated from targeting a military objective (whether it is physical or entirely made of code) and the ‘incidental loss of life, injury to civilians, damage to civilian objects, or a combination thereof’ expected from the operation.[[451]](#footnote-451) Suppose that, in order to destroy Stuxnet’s code, it is necessary to launch a cyber-operation that will also affect civilian networks and systems, causing some degree of physical violence. Since the code would not be considered a military objective, it will not be possible to determine the military advantage gained from destroying or interfering with the code, and any proportionality assessment will however be precluded. Clearly, this is not an acceptable legal outcome. At this point, a possible rebuttal would be to argue that a military objective should be defined at the level of the physical structure (for instance, the hardware) in which the data is stored. For instance, in the above example the military objective would not be considered Stuxnet’s code, but the physical structures of the affected system in which Stuxnet’s code is stored. [[452]](#footnote-452)The belligerent who is planning to launch the cyber-attack should then determine whether the hardware, and not the code, constitutes a military objective and whether or not any incidental damage to the hardware would be considered excessive to the military advantage expected from the cyber operation, in accordance with the principle of proportionality. Yet, I do not think that this approach would maximize the protection of the civilian population from a cyber-attack in the way that qualifying digital data as objects would do. As already pointed out by Heather Harrison-Dinniss, this depends by the fact that the vast majority of cyber infrastructures used by modern militaries are essentially civilian in nature, which means that they could be qualified as a military objective by virtue of their use (see *infra* para. 3.3). Once this happens, any remaining effects on the civilian function of the object must be scrutinized under the rules on proportionality and precaution.[[453]](#footnote-453) The specific amount of civilian function retained by the military objective depends essentially on the level at which the military objective itself is defined. If we return to the example examined above, any damage caused to the physical hardware in which the code of the Stuxnet malware is stored will not be considered as incidental damage but will be factored in the damage caused to the military objective. In other words, it will be left outside the proportionality equation. If, instead, the code itself is designed as a military objective, the hardware in which the code is stored could be considered as a civilian object and any damage to it should be considered within the proportionality equation as incidental damage.[[454]](#footnote-454) Secondly, the level of specificity at which a military objective is defined directly impacts the application of rules of precautions in attack. As we shall see in greater detail in Chapter 6, the rules on precaution require those who plan or decide upon an attack to minimize collateral damage both in the choice of means and methods of attack,[[455]](#footnote-455) as well as when a choice is possible between different military objectives yielding a similar degree of military advantage.[[456]](#footnote-456) If the military objective is designed at the hardware level and not at the code level, belligerents will not be in compliance with the obligation to take all feasible precautions to minimize collateral damage.[[457]](#footnote-457) For such reasons, I believe that the inclusion of digital data within the notion of ‘object’ can ensure the proper application of the principle of distinction in the cyber domain, thus ensuring adequate protection to the dignity of the civilian population.

## 2. Effective contribution to military action.

Having clarified this, we turn now to an examination of the components of the notion of ‘military objective’, in order to examine under what are the requirements that need to be in place to lawfully target an object with a cyber-attack. The first segment of Art. 51 AP I requires that an object makes an ‘effective contribution to military action’ due to its nature, location, use or purpose in order to be qualified as a military objective. In this regard, the notion of ‘effective contribution to military action’ poses two different interpretive issues. First of all, it is not clear to if the object must make an effective contribution to the military action of the defending side or to the attacking side. As such, Oeter argues that ‘effective contribution to military action’ is an ‘objective’ requirement, since it expresses the capacity of an object to effectively contribute to the military operations of the adversary.[[458]](#footnote-458) Conversely, an alternative approach argues that the text of Art. 52 (2) API can be read extensively, as to include ‘effective contribution to military action’ related to the attacker’s own side, such as ‘an area of land that one intends so capture’, which ‘will be effectively contributing, because of its location, to one’s side military action’. This interpretation conflates the notion of effective contribution to military action with the concept of ‘direct military advantage’ and is therefore legally incorrect, since the two concepts are not synonymous but need to be satisfied cumulatively.[[459]](#footnote-459) The second issue relates to how the notion of ‘military action’ should be interpreted. The use of this choice of words is the result of careful negotiations at the drafting of the 1977 conference that lead to the adoption of the Protocols, which, as we shall see, reflected the interpretive troubles inherent in the relationship between military necessity and the protection of human dignity. As noted by Neale[[460]](#footnote-460), an early draft of (then) Art. 43 made by the ICRC defined military objectives as those objects ‘which, by their nature or use, contribute effectively and directly to the military effort of the adversary, or which are of a generally recognised military interest.’ [[461]](#footnote-461) The focus of the definition was on the concepts of “military effort” and “military interest” which, coupled together, made the notion of military objective too imprecise. Eventually, the text included in the final version of Art. 52 (2) API referred only to the concept of “military action”. In clarifying its meaning, it is helpful to compare it to other notions that were considered and rejected in earlier negotiating phases, namely “military operation”, “war effort” and “military effort”. A military operation was qualified as a “movement of attack or defence by armed forces” and is the narrowest of the three proposed terms.[[462]](#footnote-462) Conversely, the notion of ‘war effort’ included ‘all national activities which by their nature or purpose would contribute to the military defeat of the adversary’, thus encompassing military and non-military activities conducted by members of one of the parties to a conflict, with the overall aim of supporting the war, and may ‘involve activities that have no connection to the actual prosecution of hostilities’.[[463]](#footnote-463)Defined as such, wareffort is an extremely broad concept which allows belligerents an almost absolute discretion in the selection of targets. Finally, ‘military effort’ was defined as ‘all the activities that are objectively useful in defence or attack in the military sense, without being the direct cause of damage inflicted, on the military level’.[[464]](#footnote-464) The concept of ‘military effort’ is more restrictive than ‘war effort’ because it encompasses only operations ‘undertaken by armed forces as part of the overall war effort’, comprising both direct and indirect connections to military operations.’[[465]](#footnote-465) The fact that the drafters of the Protocols rejected the concept of military effort denotes that the term military action employed in Art 52 (1) was seen by the drafters of the Protocols as a ‘more definite and precise standard’[[466]](#footnote-466). Thus, the resulting interpretation of the notion of ‘military action’ should be interpreted as including ‘the conduct of one or more military operations by armed forces in the prosecution of hostilities in a specific armed conflict’, [[467]](#footnote-467) and is not limited to tactical operations but covers also operational-level conduct. Having said that, State practice has shown how the concept is difficult to apply with certainty and is subject to interpretations which are way more expansive than the one just detailed above.

### 2.1. War-sustaining function and war-fighting capabilities.

One of the most contentious issue in this regard relates to the targetability of objects that perform a war-sustaining function, such as infrastructure that generates revenues, or have economic importance for a party to a conflict. Examples of State Practice are abundant, and range from the targeting of oil refineries by the US army during the Second Gulf War,[[468]](#footnote-468) , as well as in the context of anti-Isis military operations,[[469]](#footnote-469) to the bombardment by Israel of chicken farms, egg factories and food processing plants in Gaza,[[470]](#footnote-470) or the targeting of many commercial, industrial and agricultural buildings and installations, during the 2006 armed conflict between Israel and Lebanon.[[471]](#footnote-471) This practice has been justified by the attempt made by the US to equate the notion of ‘military action’ with those of ‘war-fighting’ and ‘war-sustaining’ capabilities, as exemplified by the US *Commander’s Handbook on the Law of Naval Operations*, which defines military objectives as ‘combatants, military equipment and facilities […] and those objects which, by their nature, location, purpose, or use, effectively contribute to the enemy’s war fighting or war-sustaining capabilities’[[472]](#footnote-472). This view that has been reiterated several times, as in the 2013 Joint Targeting Doctrine and in the 2016 US Law of War Manual.[[473]](#footnote-473)

 In support of its approach, the US mentions, among others, the destruction, by the Confederate Army, of raw-cotton fields belonging to the Union Forces during the American Civil War, on the grounds that the sale of cotton provided funds for almost all Confederate arms and ammunition.[[474]](#footnote-474) A similar line of reasoning has been endorsed by the Eritrea-Ethiopia Claims Commission in relation to the bombardment of the Hirgigo power plant by the Ethiopian Air Force during the Ethiopian-Eritrean war in May 2000. According to Ethiopia’s own assessments of the facts, the Hirgigo power plant was not the intended target of the attack, which was directed against two anti-aircraft missile launchers in the vicinity of the plant. The Commission ruled that the power station could qualify as a military objective, stating that, *inter alia*, one of the grounds by which the power station could be attacked was because it was of economic importance to Eritrea.[[475]](#footnote-475) Clearly, equating the notions of ‘war-fighting’ and ‘war-sustaining’ capabilities with the notion of ‘military action’ is not acceptable, because the terms are not synonymous with each other. If anything, it is possible to construe the meaning of the term ‘war-fighting’ as similar to ‘military action’, because there needs to be a direct link between the object in question and the conduct of military operations by the adversary. Thus, an ammunition factory may be considered as making an effective contribution to war-fighting, and therefore to military action, because the fabrication of ammunition is directly correlated with the military operations carried by the adversary. Conversely, the concept of ‘war-sustaining capability’ leads to a much broader interpretation, *de facto* allowing belligerents to enjoy an almost unlimited leeway as to what objects could be targeted if military necessity requires so, since ‘almost every civilian activity might be construed by the enemy as indirectly sustaining the war effort (especially when hostilities are protracted)’.[[476]](#footnote-476) Furthermore, this approach is particularly troublesome when transposed to the cyberspace, where the list of targets that could be targeted by a cyber-attack could be greatly increased, at the expense of the protection of the civilian population. To better illustrate why, consider a situation where State A is in an international armed conflict against State B, and decides to qualify as a military objective the pipelines and refineries of a State-owned oil company, solely on the basis of their war-sustaining function, since the oil production and distribution can generate revenues which may be used for purchasing weapons and military-related equipment. If we consider war-sustaining objects as being military objectives, this means that State A, in an attempt to halt the oil production of the company, can employ a Stuxnet-type attack aimed at physically damaging the pipelines and the refineries owned by the company. Clearly, qualifying war-sustaining objects as military objectives is an interpretation that should be rejected, because it departs from human dignity-based considerations in favour of an over-permissive view of military necessity and which, in turn, can have negative repercussions if applied to cyberwarfare scenarios.

### 2.3. The notion of effective contribution to military action in the cyber domain: concluding observations.

In light of these considerations, and consistently with the objective of ensuring the protection of the dignity of the civilian population, the notion of effective contribution to military action must be interpreted very narrowly in the cyber context. That is, there must be ‘a proximate nexus to the military action (or ‘war-fighting’)’[[477]](#footnote-477) of the adversary and the object that has to be targeted by a cyber-attack. Therefore, only cyber-objects that perform a war-fighting function due to their nature, location, use or purpose can be considered as military objectives, whereas objects in cyberspace that merely serve a war-sustaining role cannot be attacked and, thus, must be regarded as civilian objects. In practice, this would mean that a network which is used by the army of the adversary for the transmission of information relevant to military operations could fall within the scope of Art. 51 (API), because it has a direct link to the military action of the attacked State, considering that the disruption of the functionality of the network will break the chain of communication and slow down the enemy. Similarly, an electrical power grid servicing an ammunition factory makes an effective contribution to military action because it is instrumental for the conduct of operation of a party to the conflict and can therefore be the target of a cyber-attack. Conversely, disabling the network of the banking system of the attacked State will amount to targeting a civilian object, and would therefore constitute a violation of the principle of distinction. That is because the banking system of a State is essentially an economic target which serves a war-sustaining function, therefore the causal link to military action would be too tenuous to satisfy the first part the test of Art. 52 (2) AP I.

## 3. The four criteria: Nature, Location, Use and Purpose.

An object can qualify as a military objective if, due to its nature, location, purpose or use, it makes an effective contribution to military action. These four criteria do not need to be cumulatively fulfilled at the same time for the object to fall within the scope of Art 52 (2), even if they can coexist at the same time. For instance, an object may qualify as a military objective both for its actual use and because of its location.
With regards to the nature requirement, if such condition is met, all other elements of the test are deemed to be satisfied.

### 3.1. Nature.

The nature criterion can be distilled into one essential quality: the intrinsic feature of the object, from which its effective contribution to military action is derived. In other words, the object possesses some inherent military qualities, related to its application and function, which make it intrinsically contributing to military action.[[478]](#footnote-478)Examples of objects that are intrinsically military in their nature include, first of all, those objects that cannot be used for other purpose beyond a military one, such as military operational plans, fortifications, entrenchments, military equipment and weapons of all types. In the cyber context, the notion extends to military computer, military cyber infrastructures, so called ‘C4ISR’ systems (that is, command, control, communications, computer, intelligence, surveillance and reconnaissance), as well as ‘the facilities in which these computers, infrastructures and systems are permanently housed’. [[479]](#footnote-479) Furthermore, the notion extends to cyber-weapons, such as malware designed to launch ‘attacks’ against the adversary. Clearly, it is worth reminding that the notion of attack I am referring to consists of malware which results not only physical violence, but also severe psychological violence or severe economic violence.

The nature criterion is not only limited to objects which intrinsically contribute to military action but can be extended to those objects which are specifically designed to be used for military purposes only. Within this sub-category we can include barracks, military units, ammunition deposits, military ports and docks, military aircraft and airfields. As far as the cyber context is concerned, this would include military computers, network and the use of which is exclusively military.

A separate question revolves around the practical limits of applicability of the requirement. As such, the ICRC has taken the view that the concept of ‘nature’ extends to ‘all objects directly used by the armed forces’. Such interpretation it untenable, since it conflates the ‘nature’ requirement with the requirement of ‘use ‘and would render the former concept redundant: as explained *supra*, the nature requirement relates to the intrinsic military character of the features of the object in question, irrespective of their actual use. In addition, such interpretation leads to some uncertainty with regards to the qualification of peculiar objects: for instance, Dinstein notes that ‘power plants serving the military’ are all military objectives because their nature makes an effective contribution to the military action of the adversary. In the cyber domain, this would extend to all the SCADA systems and networks operating such power stations. While power plants serving the military do fall within the scope of Art 52 (2) AP I, it is so because of their use, not by their intrinsic features. Similar concerns arise with regards to lines of communication and transportation (‘LOCs’) which are routes connecting a military force with a base of operations. These objects include ‘arteries of transportation of strategic importance, principally mainline railroads and rail marshalling yards, major motorways, navigable rivers and canals’,[[480]](#footnote-480) and, as far as the cyber domain is concerned, underground and undersea communication nodes and cables, computer and computer networks used by the armed forces.

The present author does not believe that LOCs should be considered as satisfying the nature requirement, as the fact that some LOCs are of ‘strategic importance’ or are military relevant does not have any significance with regards to their ‘nature’, but can be considered as being a consequence of their location or their use, two requirements that will be discussed *infra*. This consideration, however, does not extend for those LOCs which were deliberately built to serve military forces and were exclusively utilised by them, such as cables and nodes of communication.

### 3.2. Location.

With regards to the location requirement, its *rationale* is that a civilian object may make an effective contribution to military action due to its geographical situation, ‘either because it is a site that must be seized or because is important to prevent the enemy from seizing it, or otherwise because it is a matter of forcing the enemy to retreat from it’[[481]](#footnote-481). Primary examples of military objectives by location include, as mentioned *supra*, LOCs (lines of communication and transportation) as well as certain pieces of land and buildings – such as a mountainous pass or a monastery on top of a hill the control of which is of tactical importance to the belligerents. This means that such objects can be targeted by cyber-attacks. Consider, for instance, the example provided by the Tallinn Manual 2.0, where the SCADA system of a reservoir is targeted by a cyber-operation in order to ‘release waters into an area in which military operations are expected, thereby denying its use to the enemy.’ In this case, according to the Tallinn Manual, ‘the area of land is a military objective by location because of its military utility to the enemy’.[[482]](#footnote-482)Beyond that, certain type of physical cyber infrastructure can satisfy the location requirement, such as undersea cables, the nodes of a telecommunication networks, a Wi-Fi network located in an area where the enemy is operating.Therefore, there might be instances in which the opposing party is relying on a network node for their communication, so that it makes an effective contribution to military action and destroying it, or disrupting its functionality, may offer a definite military advantage. A separate point revolves virtual objects, that is, *digital data* that operate or are stored within a physical infrastructure. Clearly, data can be targeted by their location, to the extent that they are associated to the location of a specific physical cyber-infrastructure.

To illustrate my point, consider the question related to the physical targetability of computer networks. To begin with, we can certainly argue that an object can qualify as a military objective by virtue of its network location alone, rather than by its location in the physical space. As such, a ‘civilian Wi-Fi network located in an area in which an enemy is operating may enable the enemy to’ piggy-back communication of the signal’, therefore it can be assumed that such network makes an effective contribution to military action due to its location, because ‘denying the enemy use of the network may give a concrete and direct advantage to the attacking forces.’[[483]](#footnote-483)

### 3.3. Use and Purpose.

With regards to the requirements of ‘use’ and ‘purpose’, both of them are fairly similar in their underlying assumptions: while use is related with the object’s present function, the object’s purpose is concerned with its intended future use, which can be deduced from an established intention of the belligerents as regard such future use. Such intention, moreover, must be not be based on contingency plans that take into account ‘worst-case scenarios’: doing otherwise would render the ‘purpose’ requirement over-inclusive and ultimately useless, as every object could be construed as being a military objective in light of its hypothetical future use, no matter how unlikely it might be in the future. In the cyber context, this means that a computer system or network constitutes a military objective, for instance, if it is used for launching a cyber-operation rising to the level of an attack under Art. 48 AP I. It must be pointed out, however, that in case of doubt over whether an object which is normally a civilian one is being used to make an effective contribution to military action, Art. 52 (3) mandates a presumption that it is not. Moreover, an additional *caveat* relates on the fact that use and purpose are temporally limited requirements: much like direct participation in hostilities, a computer that is being used to launch a cyber – attack will retain its status as a civilian object as long as the attack has ended, making it immune from being targeted. Furthermore, an important question revolves around the targetability of ‘dual use’ objects, a concept employed to describe those objects which perform both a civilian and a military function, such as an electricity grid whose power supplies both a civilian area and a military base. For instance, an electrical power grid can qualify as a military objective and be targeted by a computer-network attack because, despite it being civilian in nature, it could make an effective contribution to military action by serving the military and its destruction, capture and neutralization may offer a definite military advantage. Other dual-use objects in the cyber context include civilian computer networks being used by the military as well as technologies such as the Global Positioning System (GPS) which have been integrated in many civilian applications. A specific issue, in this regard, relates on whether the Internet can be qualified as a military objective in its entirety, and whether belligerents can shut down internet communications at a large scale. Although there are no examples of State practice related to situations of armed conflict, there have been a few instances when, in times of internal unrest, governments have shown their willingness to shut down Internet networks on a nation-wide scale. For instance, Nepal and Myanmar shut down their internet connection in response to national unrest in 6 and 2007. [[484]](#footnote-484) Similarly, in 2011 protests erupted in Egypt where confronted by the Mubarak Government with a five-day shutdown of the Internet networks in an attempt to curb down the protests.[[485]](#footnote-485) Finally, as recently as November 2019, internet communications were cut-off in Iran as protests against the government were escalating in intensity.[[486]](#footnote-486) The question that arises, then, is whether the large-scale targeting of a civilian network would be lawful under IHL. To begin with, it must be pointed out that there must be a causal link between the use of the internet as an object and its effective contribution to military action. To put it differently, what would need to be proven is the relationship between the use of the internet as a whole and its relevance for the military operations carried out by the armed forces of the enemy. For instance, the internet could be an integral part of the enemy’s communication system, so its use would make an effective contribution to military action. Under this circumstance, a cyber-operation that targets the internet will be a lawful attack under the *jus in bello*. Conversely, if the internet is used for propaganda purposes or, say, to share information about protests erupting in a State, it is not *used* in such way that it makes an effective contribution to military action, which is a term that has to be defined narrowly. Similarly, the Internet cannot be attacked simply because it is of economic value for the enemy, since this would legitimize targeting war-sustaining object and, as explained *supra*, this would make the application of the principle too far reaching and would give the attacker too much discretion. Beyond that, the main issues when targeting dual-use objects revolve, firstly, around the application of the principle of precaution, to determine if the object in question can be targeted by kinetic means or cyber means. Secondly, the principle of proportionality must be assessed, to avoid any damage, whether in the form of death or injury to civilians or damage of destruction to objects, that is excessive compared to the military advantage expected from the operation.

## 4. Definite Military Advantage.

The second part of the test for qualifying an object as a military objective requires that its destruction, capture and neutralization must offer, in the circumstances ruling at the time, a definite military advantage.[[487]](#footnote-487)The concept of definite military advantage is closely connected with the notion of effective contribution to military action. While the latter concept is referred to as an ‘objective’ criterion, the notion of definite military advantage has a ‘subjective’ element attached to it, since it represents the attacking party’s assessment towards the achievement of a military gain.[[488]](#footnote-488)

 In this regard, it has been argued that what Art 52 (2) requires is cumulativesatisfaction: in other words, what suffices is that the two requirements are both satisfied, even if not at the same time. As such, the destruction, capture of neutralization of an object can make an effective contribution to military action but the definite advantage gained from its destruction, capture or neutralization can arise later. For instance, Henderson notes, by referencing to an attack to a computer system, that ‘it is arguable that damaging or destroying the system would be of benefit only in the longer term – as arguably the enemy’s current operations and even short-term plans would continue.’ [[489]](#footnote-489) This interpretation is not entirely persuasive, as it can be pointed out that the requirement of military advantage is satisfied the moment a certain object is destroyed or neutralized by an attack. In light of this consideration, it can be submitted that what is needed to satisfy the definition of military objective is the *simultaneous* satisfaction of both the requirement of effective contribution to military action and definite military advantage. This interpretation holds even more strength in the cyber domain: consider, for instance, when a civilian computer network is used by the armed forces of a party to a conflict. In this case, the object can be said to make an effective contribution to military action as long as the computer network is being used by the military, otherwise it will regain its status as a civilian object and no definite military advantage would result by its destruction, capture or neutralization. The definition of ‘military advantage’ requires the existence of a clear nexus between the object in question and ongoing or planned military operations in a specific armed conflict. Very much like the concept of ‘effective contribution to military action’, the quantification of this belligerent nexus has been subjectto various interpretations. The most liberal interpretation has been offered by the EECC in its assessment on the lawfulness of the bombardment of the Hirgigo power plant by Ethiopian forces, where it noted that:

‘[…] the fact that the power station was of economic importance to Eritrea is evidence that damage to it, in the circumstances prevailing in late May 2000 when Ethiopia was trying to agree to end the war, offered a definite advantage. ‘The purpose of any military action must always be to influence the political will of the adversary.’[[490]](#footnote-490)

The above-mentioned approach is in line with the EECC’s interpretation of the notion of effective contribution to military action, as it includes not only military gains but also purely political ones. As observed by Dinstein, ‘a potential political outcome is not an admissible consideration in assessing the character of the object as a military objective. And ‘forcing a change in the negotiating attitudes of the enemy ‘cannot be deemed a proper military advantage.’[[491]](#footnote-491)

At the other hand of the spectrum there is the ICRC approach, according to which ‘a military advantage only can only consist in ground gained and in annihilating or weakening the enemy armed forces.[[492]](#footnote-492) The ICRC’s position is definitely the most balanced of the two, but it needs to be taken with the added *caveat* that the weakening of the enemy’s armed forces ‘does not comprise only killing the adversary’s combatants’[[493]](#footnote-493), but extends to ‘weakening the enemy’s war fighting and defending capability’[[494]](#footnote-494). This includes actions such as damaging a steel plant that produces parts for military planes or, in the cyber domain, disrupting an enemy’s network to interrupt its communications.

Finally, the military advantage gained from the attack needs to be definite, that is, concrete and perceptible rather than purely hypothetical or speculative.[[495]](#footnote-495) However, this does not mean that the definite military advantage is limited to tactical gains; on the contrary, it extends to the estimation of the long-term and large-scale military benefit of an attack.[[496]](#footnote-496) The assessment of the concept of definite military advantage does not pose peculiar challenges to cyber warfare, other than some overly expansive interpretations, such as the one endorsed by the EECC, that however do not represent the States’ view on the matter. What is more relevant in the cyber context is how to interpret the methods needed to obtain a military advantage, namely destruction, capture and neutralization. The meaning of the first concept is quite straightforward and includes any action that compromises the essential features of a physical object – or a virtual one, in the case of digital data- in order to make the object unusable to both sides of the conflict. The notion of ‘capture’, instead, is ‘gained from acts of seizing and maintaining control or possession of object’,[[497]](#footnote-497) and it is aimed at denying the object’s effective contribution to military action to the other side of the conflict. Lastly, ‘neutralization’ requires disabling an object since it is incapable of functioning as intended:[[498]](#footnote-498) while the meaning of this concept is akin to that of ‘destruction’, neutralization bears a significant relevance in cyber-warfare, since many cyber-operations are capable of disrupting the functionality of an object, thereby ‘neutralizing’ it. In this regard, it is worth noting that choice of the method by which a belligerent can achieve a definite military advantage when targeting a military objective will be dictated by the precautionary requirements laid down under Art. 57(2) (ii)AP I, according to which belligerents must ‘take all feasible precaution in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects’.[[499]](#footnote-499)However, we shall see that the protective scope of Art 57 (2) (ii) AP I is rather limited, since the balance between the protection of human dignity and military necessity considerations under Art. 57 (2) (ii) AP I is strongly tilted in favour of the latter principle. In fact, the obligations set out by the article only arise when a belligerent would acquire the same military advantage between different methods of achieving it: in other words, while neutralizing an object through a cyber-attack would be in compliance with Art. 57 (2) (ii), it is highly doubtful that such method would yield the same military advantage of destroying the same object, either through a CNA or using kinetic means. For this reason, at the present time does not exist any ‘duty to hack’ an object *in lieu* of destroying it, and such a position remains a matter of *lege ferenda*.[[500]](#footnote-500)

## 5. Conclusion.

The Chapter has discussed the application of the principle of distinction between military objectives and civilian objects in the cyber context. The greatest interpretive challenge is represented by whether one considers *digital data* as qualifying as an object for the purposes of Art. 52 (2): in this regard, the Chapter has demonstrated how an extensive interpretation of the concept of ‘object’ would lead, on the one hand, to greater protection of the civilian population, while on the other it would allow parties to the conflict to consider *digital data* as military objective. Beyond that, legal issues revolve around the possible consequences of diverging interpretations of the elements that compose the definition of military objective, such as the criteria of nature, location, use and purpose, as well the concepts of ‘effective contribution to military action’ and ‘definite military advantage’. However, I believe that the most important practical consequence when applying the definition of military objective to cyberspace is that the scope of what can be lawfully targeted by kinetic or cybernetic means is greatly expanded. This is especially true, considering the prevalence of dual-use cyber infrastructures over military ones. Therefore, as I will discuss in the following Chapters, the application of the principles of proportionality and precaution becomes of essential importance for the purpose of humanizing the conduct of hostilities in cyberspace and for protecting the dignity of the civilian population.

# Chapter V. The Principle of Proportionality in Cyber Warfare and its applicative issues with regards to the relationship between the principles of military necessity and humanity.

Although the word ‘proportionality’ does not appear in any of the treaties of the law of armed conflict, it is commonly acknowledged that the principle is enshrined in the rules of API prohibiting indiscriminate attacks and in those related to precautions in attack, as well as in the Rome Statute of the International Criminal Court. As such, Art.51 (5) (b) qualifies as indiscriminate an attack which may be expected to cause excessive *collateral damage*, that is, ‘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.’[[501]](#footnote-501)The same wording is repeated under Art 57. 2 (a) (iii) and (b) of AP, which imposes an obligation to refrain from launching (or cancel or suspend) attacks which are expected to cause excessive collateral damage.[[502]](#footnote-502) Furthermore, Art. 8 of the Rome Statute uses an almost identical language to Art. 51 AP I when listing indiscriminate attacks among the list of war crimes, with the notable difference that it applies only to those attacks that are expected to cause collateral damage in a way which would be ‘clearly excessive in relation to the direct and concrete overall military advantage anticipated.’[[503]](#footnote-503) The principle of proportionality possesses the status of customary international law,[[504]](#footnote-504) is applicable to both international and non-international armed conflicts,[[505]](#footnote-505) and it performs an essential role in the *jus in bello*. As discussed in Chapter 1, the rules on proportionality are the logical outgrowth of the principle of distinction, as they both serve a similar regulatory function. While the principle of distinction determines who and what can be lawfully attacked, distinguishing civilians and civilian objects from combatants and military objectives, the principle of proportionality assumes that civilian suffering in armed conflict is unavoidable, and therefore aims at restricting the amount of violence that belligerents can employ when they are attacking a lawful target. As a ‘method of regulation of the level of violence in armed conflict’,[[506]](#footnote-506) the rules on proportionality require to compare the expectation of collateral damage against the military advantage anticipated from an attack, and, when the latter exceeds the former, to qualify the attack as unlawful. As such, the principle of proportionality is where the tension between military necessity and the principle of humanity is most vivid. It comes as no surprise, then, that the principle is notoriously difficult to assess on the battlefield: as succinctly pointed out by the *Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* in its *Final Report*, ‘the main problem with the principle of proportionality is not whether or not it exists but what it means and how it is applied’.[[507]](#footnote-507) Such a statement is derived from the consideration that many of the present day armed conflicts are fought in urban theatres; in these scenarios, there is a very high likelihood that military objectives could be situated in a densely populated area, resulting in attacks causing high number of civilian casualties and extensive destruction; or the targeted military objective could be a dual-use object, in that it performs both a military and a civilian function, such as an electrical power plant supplying energy both to a military compound and a civilian neighbourhood. In similar situations, it becomes particularly difficult to evaluate the effects arising from the attack against the expected collateral damage. Therefore, scholars, States and Tribunals have been divided on numerous issues related to the principle of proportionality, since its codification under the rules of AP I; questions are raised in relation to the exact scope of application of the elements of the proportionality analysis, such as the degree to which a military commander must foresee incidental damage, the extent to which ‘reverberating’ effects should be accounted for, and what is the meaning of ‘concrete and direct military advantage’. Moreover, the very logic of the principle has been criticized because requires making a balance between two values, collateral damage and military advantage, which are intrinsically incommensurable and therefore not measurable against each other. In this regard, the application of the principle of proportionality to cyber warfare adds an additional layer of complexity to the proportionality equation, given the high degree of interconnectivity between military objectives and civilian objects in cyberspace, as well as the potential of cyber-attacks causing reverberating effect which may be difficult to predict with sufficient precision. In light of these consideration, the aim of the Chapter is to discuss the principle of proportionality, as it is applied to cyber-warfare, through the *lens* of the dynamic between the principle of humanity and that of military necessity. In order to do so, Section I of the Chapter will begin with an examination of the first element of the proportionality analysis, the concept of collateral damage and its components (that is, death or injury to civilians, damage to civilian objects). More specifically, two claims will be made: firstly, that knock-on effects of cyber-attacks must also be taken into account in the proportionality assessment, but only to the extent that they are foreseeable by a reasonable military commander; secondly, that the proportionality rule must consider as ‘damage to civilian objects’ not only destructive effects from cyber-attacks, but also other kind of effects, such as psychological and economic harm. Section II then proceeds with an analysis of the second limb of the proportionality rule, the concept of ‘concrete and direct military advantage anticipated’ from the cyber-attack. In this regard, the section will discuss how to assess ‘immediacy’ and ‘directness’ in the cyber context; what is the degree of anticipation arising from a cyber-attack; finally, whether or not the notion ‘force protection’ – that is, minimizing the risk to life of the forces of the attacking party to the conflict – can be considered as constituting a military advantage when launching cyber-attacks and, if so, what consequences does it bear for the military necessity-humanity dynamic. Finally, Section III of the Chapter discusses the issues related to the comparison between the two prongs of the proportionality analysis, collateral damage and military advantage, exploring the consequences of the indeterminacy inherent in this comparison in the cyber context.

## 1. Evaluating Collateral Damage in the Cyber Domain.

Before analysing the issues raised by the first prong of the principle of proportionality, it is necessary to discuss the impact of two preliminary issues, namely under what circumstances does the principle of proportionality apply, and in relation to what kind of acts.

### 1.1. Applying the principle of proportionality in cyber: what kind damage counts in the proportionality assessment?

It is commonly understood that the principle of proportionality is only concerned with damage to civilians or civilian objects which is ‘incidental’, as it may result from attacking a lawful target.[[508]](#footnote-508) As a textbook example, consider the bombardment of a military barrack located in a civilian area: under this scenario, even if civilians are likely to be injured or killed, and civilian objects likely to be destroyed, what matters is that they are not the actual target of the attack, but have to factored in the proportionality analysis as an unavoidable cost of conducting military operations. Conversely, damage which is ‘intentional’ results from directly attacking the civilian population or civilian objects. In this situation, the conduct in question constitutes a grave breach of the Geneva Conventions and may give rise to international criminal responsibility, therefore the principle of proportionality is not engaged. Secondly, the principle of proportionality does not concern damage suffered by combatants or civilian directly participating in hostilities, since they qualify as legitimate military targets:[[509]](#footnote-509) therefore, opposing forces may employ any amount of force against them, barring the prohibition on using means and methods of warfare that cause superfluous injury or unnecessary suffering.[[510]](#footnote-510) A more complex question is if, and to what extent, does the principle of proportionality apply to military objectives. As discussed in Chapter 3, military objectives are those objects which by their ‘nature, use, location or purpose make an effective contribution to military action and whose capture, destruction or neutralization offers a definite military advantage.’[[511]](#footnote-511) There is no doubt that the targeting of a military objective by nature, such a military aircraft, does not impose any proportionality assessment by the attacking party; however, issues arise when it comes to targeting dual-use objects, that is, objects that are civilian in nature but that can become military objectives due to their use, location or purpose. According to one approach, dual-use objects are protected by a ‘limited’ version of the proportionality principle.[[512]](#footnote-512) Once a dual-use object qualifies as a lawful target by use, location, or purpose, it becomes a military objective in its totality: therefore, ‘the civilian contributions made by dual-use facilities simply evaporates from the analysis […], and only incidental harm to civilians and civilian objects is taken into account in making proportionality assessments.’[[513]](#footnote-513) A different interpretation, proposed by Shue and Wippman, suggest that dual-use objects should benefit from what they called ‘enhanced proportionality’, whereby the destruction of the civilian function of a dual-use object should be considered in the proportionality test, including any reverberating effects caused by the attack.[[514]](#footnote-514)

The two positions yield dramatically different results when applied to the cyber context. Consider, for instance, the targeting of a dual-use object such as the controlling system of an electrical power grid that provides energy to a civilian neighbourhood and to a military training site. Under the limited proportionality approach, the physical destruction of the power grid would fall outside the scope of the rules of proportionality, which would only apply to the hypothetical death of civilians or to damage caused to civilian objects resulting from the foreseeable reverberating effects caused by the cyber-attack, such as the spread of fires following a power outage. Given the very high degree of interconnection that exists between civilian and military networks, and the fact that many civilian objects may turn into military objectives in cyberspace, the ‘limited proportionality’ interpretation allows the attacking party to launch cyber-attacks with little legal scrutiny, and has the potential to magnify, rather than reduce, the adverse effects caused by cyber warfare on civilian objects and the civilian population. Conversely, the ‘enhanced proportionality’ approach has to be preferred not only since it is represented in the majority of the doctrine,[[515]](#footnote-515) as well as modern State Practice, including the US, [[516]](#footnote-516) but also because it is consistent with how the concept of military objective has been interpreted with regards to dual-use objects; in fact, as discussed in Chapter 3, once an object qualifies as a lawful target of attack due to its use, location of purpose, it nonetheless retains its civilian character, thus falling under the protective scope of the principle of proportionality.[[517]](#footnote-517) In practical terms, the adoption of a proportionality standard that adds more restraints on the targeting of dual-use facilities would consequently ensure a greater degree of protection to the civilian populations and civilian object, in a way which is consistent with the human dignity inspired values of IHL.

### 1.2. The notion of ‘attack’ as a precondition for the application of the rules on proportionality.

The second preliminary issue relates to the fact that the principle of proportionality applies to ‘attacks’. In this regard, Art. 51 (2) (5) (b) qualifies as indiscriminate *an attack* that causes excessive collateral damage, and, in a similar vein, Art. 57 requires belligerents to suspend or cancel *attacks* that would manifestly cause excessive collateral damage. As far as conventional warfare is concerned, the notion of attack is easily reconcilable with the effects that are expected to be caused by military operations in which kinetic weapons are employed, that is, *physical violence* in the form of death or injury to civilians and/or damage to civilian objects. Any other operation that does not cause physical violence, such as intelligence gathering or reconnaissance operations, do not constitute an attack and are not subject to the rules on proportionality. In this way, the rules of proportionality take into account both the needs of the belligerent parties, for whom launching attack is necessary to accomplish their military objectives, as well as the humanitarian imperative to limit the effects of the attacks against the civilian population in order to protect human dignity in its core component of physical integrity, mental integrity and wellbeing.

The cyber context, however, is quite different: in fact, cyber operations can cause a variety of effects, some of which may be qualified as physical violence, while others would fall outside its scope. It would be incorrect, however, to argue that only cyber-operations causing death or injury to civilians or damage to objects can be considered as attacks to which the principle of proportionality applies: as submitted in Chapter 2, the threshold of physical violence as a qualifier of what is an attack is too restrictive and should be abandoned, as far as cyber-warfare is concerned. Instead, I have argued in Chapter 2 how the concept of cyber-*attack* should be interpreted more broadly, to include also those cyber operations that serious psychological violence and serious economic violence. Thus, for instance, a cyber-attack against a Critical National Infrastructure would fall under the category of ‘attack’ regardless of whether it caused physical violence or not. As a consequence, an expansive interpretation of the notion of ‘attack’ in the cyber context leads, in turn, to a broader application of the rules of proportionality in the cyber domain. We shall see how this endeavour can be legally problematic, given the textual limits of Art 51 (5) (2) (b) of Additional Protocol I, which considers collateral damage only in the form of death or injury to civilians, or damage to objects. Having premised this, the next paragraph will discuss the issues raised by applying the first prong of the proportionality analysis to cyber-attacks.

### 1.3 The notion of ‘incidental harm’ in the cyber context: are reverberating effects of cyber-attacks included in the proportionality analysis?

The rules on proportionality require belligerents to evaluate incidental damage which may be expected from the attack: in other words, they do not require an ex post facto judgment, but an a priori assessment. In the cyber context, one important question relates to the meaning of the words ‘may be expected’ and whether they should be interpreted as taking into account only first-order consequences of attacks or if they include also reverberating effects.

For the purposes of the present argument, it is worth reminding that the effects resulting from an attack can be distinguished between first order (or ‘direct’ effects) and second order (also known as ‘indirect’ or ‘reverberating’ effects). First order effects take place, in the chain of causation, as ‘the immediate, first order consequences of an attack, unaltered by intervening events or mechanisms.’[[518]](#footnote-518) In the case of a cyber-attack, they are the product of the interaction between the specific tools used to launch the cyber-attack and the target network or system, and result in data disruption or alteration. Conversely, indirect effects are ‘the delayed and displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms’[[519]](#footnote-519). For instance, a cyber-attack that disables the control system of a power grid (which is the first-order effect caused by the attack), may produce reverberating effects in the form of physical damage (a fire that spreads following the power outage), or non-physical damage, such as economic harm (the cost of putting the power grid back in its full operative capacity) or other forms of disruption (the power outage can adversely impact the welfare of the civilian population in different ways, by depriving them of electricity, for instance).In this regard, it must be pointed out that first-order effects of cyber-attacks fly under the scope of the jus in bello. In fact, even considering data as ‘objects’ under IHL,[[520]](#footnote-520) it can be argued that destroying or damaging data does not suffice, in and of itself, to qualify the cyber-operation as an ‘attack’ to which the rules of proportionality would be applied, given that first-order consequences merely happen in the virtuality of cyberspace. What instead matters, for the purposes of the *jus in bello*, is the fact that first-order consequences of cyber-attacks may produce, in the physical world, reverberating effects that reach a certain threshold of intensity (that is, physical violence, serious psychological harm, serious economic harm, or a combination thereof). Therefore, determining whether and to what extent reverberating effects should be accounted as expected collateral damage has profound consequences in the cyber context.

Generally speaking, the obligation to consider reverberating effects when applying the principles of proportionality and precaution stems, first and foremost, from interpreting the rules on proportionality and precaution in Additional Protocol I consistently with Art. 33 of the VCLT.[[521]](#footnote-521)From a purely literal standpoint, the phrase ‘may be expected’ in Articles 51(5) (b) and 57 (2) (a) (iii) and (b) of Additional Protocol I is not subject to any temporal or spatial limitations. Rather, the ICRC’s Commentary on AP I clarifies that the drafters of the Protocols expressly rejected attempts to restrict incidental damage to that in close spatial proximity of a military objective.[[522]](#footnote-522) As correctly observed by Robinson and Nohle, ‘there is accordingly no reason, based on the text of the provisions, to limit the assessments under the rules of proportionality and precautions in attack to the immediate and direct effects of an attack.’[[523]](#footnote-523) This view is further reinforced by a systematic reading of AP I, where the relevance of reverberating effects can be deduced by certain specific articles; for instance, Art. 55 demands that ‘care shall be taken to protect the natural environment against widespread, long-term and severe damage. This protection includes a prohibition of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby prejudice the health or survival of the population.’[[524]](#footnote-524) The reference to ‘long-term’ damage, more specifically, implies that secondary effects against the environment are within the scope of the provision. Similarly, other articles are focused on protecting the civilian population and objects against reverberating effects, such as Art. 54,[[525]](#footnote-525) containing a prohibition to attack, destroy, remove or render useless objects indispensable for the survival of the civilian population, and Art. 56, which requires belligerents not to attack installation containing dangerous forces, as ‘severe losses among the civilian population’ may result.[[526]](#footnote-526) In both provisions, the main point of concern is not on the damage to protected civilian objects as a first-order effect of the attack, but specifically on the second-tier adverse consequences that the civilian population may face, such as the deterioration of health and welfare that may follow from the destruction of food crops and water deposits.

In addition to purposive treaty interpretation, there is an ever-growing State Practice that recognizes reverberating effects as part of the proportionality assessment. In this regard, the Final Declaration of the Third Review Conference on the Convention on Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or Have Indiscriminate Effects (hereinafter ‘CCW Convention’), which was adopted by consensus, declared that ‘the foreseeable effects of explosive remnants of war are a relevant factor to be considered in applying the international humanitarian law rules on proportionality and precautions in attack.[[527]](#footnote-527) Beyond of this specific ambit, many military manuals now explicitly recognize that the principle of proportionality applies to reverberating effects; the US Counterinsurgency Field Manual, for instance, states that ‘leaders must consider not only the first order effects of a munition or action, but also possible second and third-order effects -even undesired ones.’[[528]](#footnote-528) In the cyber-context, the majority of the doctrine includes reverberating effects in the scope of collateral damage.[[529]](#footnote-529) In this regard, the *Tallinn Manual* clarifies that ‘the collateral damage factored in the proportionality calculation includes any indirect effects that should be expected by those individuals planning, approving, or executing a cyber-attack.’[[530]](#footnote-530)

### 1.4. What is ‘expected’ collateral damage in the cyber domain?

From the above analysis, it must be concluded that the principle of proportionality does indeed apply to second-order consequences of cyber-attacks. The *crux* of the matter, however, lies in how to interpret the word ‘expected’, which raises several issues, the untangling of which has different ramifications in cyber-warfare. A first question relates on the very nature of the assessment of the expected collateral damage and whether it is a subjective or objective task. In this regard, the US Law of War Manual notes that ‘the question of whether the expected incidental harm is excessive may be a highly open-ended legal inquiry, and the answer may be *subjective* and imprecise.’[[531]](#footnote-531) A similar conclusion was implied by the Eritrea-Ethiopia Claims Commission; the case revolved around the aerial bombardment by Eritrean forces of the Mekele Airport, which had been attacked with cluster bombs that killed as many as fifth-three civilians, and caused extensive destruction in the surrounding neighbourhood of Mekele town, including a school attended by children.[[532]](#footnote-532)

In reviewing the legality of the action, the Commission identified the governing legal basis in Art. 57 (1) Additional Protocol I, according to which the attacking party must take all feasible precautions in the choice of means and methods of warfare so as to minimize incidental harm, and to suspend or stop an attack when it becomes manifest that such attack would cause excessive expected collateral damage.[[533]](#footnote-533) While the Court was seriously concerned by the ‘lack of essential care’ in conducting the operation by Eritrea, it however seemed to endorse the view that the expectation of collateral damage, and the feasibility of the precautionary measures that must be employed to minimize it, must be assessed through the purely subjective perspective of the agent.[[534]](#footnote-534) The subjective approach tothe assessment of expected collateral damage has troublesome implications for the conduct of hostilities in cyberspace, since what matters is merely the personal situation in which the attacker is able to make the evaluation of expected collateral damage. Therefore, the attacker may choose to minimize the risk to its own life over obtaining more accurate information on the expected incidental harm resulting from the attack, if this course of action would come at a greater cost for his own personal safety. Furthermore, cyber-attacks may be the end-result of a complex process that requires the development and design of a cyber-weapon, followed by its deployment against the target network, in which different individuals may be involved. It may very well be the case that the individual tasked with launching the cyber-attack may not have the technical skills to gauge the likelihood of reverberating effects stemming from the attack, such as the risk of malicious code infecting the network of civilian infrastructures, an eventuality that happened in the case of the Stuxnet worm.[[535]](#footnote-535) Under the subjective standard, there is a risk that the assessment of the expected collateral damage in the cyber context would be considered lawful, regardless of the inexperience or ineptitude of the attacker. Consequently, the principle of proportionality would lose much of its substance and the civilian population would be deprived of an important legal mechanism for the regulation of cyber-violence in an armed conflict.

More recently, however, doctrine and state Practice have strayed away from this interpretation, leaning towards the adoption of a more objective standard. For instance, in the *Galic* case, the ICTY held that ‘in determining whether an attack was proportionate is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessivecivilian casualties to result from the attack.’[[536]](#footnote-536) While *Galic* endorsed the standard of the ‘reasonable person’, certain authors have advocated for an even higher threshold, that of the ‘reasonable military commander’ a standard which ‘requires consideration of a commander’s assessment of the expected collateral damage from an attack. The test is based on the expected collateral damage that a ‘reasonable commander’ would have assessed at the time of the attack – and not the damage that actually occurred as a result of the attack.’[[537]](#footnote-537) The advantage of this approach is that a ‘reasonable military commander’, as opposed to a reasonably well-informed person, is presumed to possess the specific information which, in the circumstances ruling at the time, are necessary to make an evaluation as to the expected collateral damage: what it means, in practical terms, is that the military commander has a legal requirement to foresee certain consequences of an attack, something which cannot be asked when the assessment is performed by a ‘reasonable person’.[[538]](#footnote-538) Since its formulation in the context of the review of the NATO bombing campaign against Yugoslavia in 1999, the reasonable commander standard has found ample support by authors, national and international jurisprudence, and most notably state practice. It can be safely argued, then, that the incidental harm resulting from an attack, including any reverberating effect, must be evaluated from the perspective of a reasonable military commander. However, this interpretation begs a further question: what kind of effects is a reasonable commander expected to foresee in the cyber context? In other words, what is the degree of causation between the cyber-attack and reverberating effects that matters, for the purposes of the principle of proportionality?

In this regard, the doctrine has proposed several alternative standards. The most restrictive interpretation has been advanced by Schmitt, Dinnis and Wingfield, who have argued that the attack must be the ‘proximate cause’ of the effects, which would not have occurred ‘but for’ the cyber-attack; by contrast, any other kind of reverberating effect that happened independently from the attack would not be relevant for the principle of proportionality.[[539]](#footnote-539) While this approach could determine with a high degree of accuracy the causal link between the attack and its effects, it seems more suitable for an *ex post facto* determination, rather than for evaluating, *a priori*, which effects may be expected as incidental collateral damage.[[540]](#footnote-540) A different interpretation has been proposed by Christopher Greenwood, according to whom *expected* means that something is ‘more likely than not’ to take place;[[541]](#footnote-541) in the opinion of the present writer, this standard can be applied to the cyber scenario, as military commanders can only be asked to account for those effect that have a high degree of probability to happen as a result of a cyber-attack. This would prevent the military commander from taking into consideration events that are too causally remote from the cyber-attack that originated them.[[542]](#footnote-542) In practice, the military commander can be assisted by specialists that will help him to correctly gauge the expected incidental harm, especially ‘by collecting information about the attacked network (network mapping) or operating system (footprinting).’[[543]](#footnote-543)

Having considered this, the duty of the reasonable military commander to foresee reverberating effects extends both geographically and temporally. In fact, there might be foreseeable reverberating effects that that take place in an area which is geographically removed from the primary target of a cyber-attack: for instance, a cyber-attack that destroys a power distribution line may be reasonably expected to cut off the water supply of a large number of civilians, not only those who live in the zone in which the target is located. Furthermore, a cyber-attack can cause reverberating effects which are temporally removed from the original operation by days, or even months. Consider, in this regard, an attack that targets an oil facility, causing the release of toxic material in the surrounding area: under this scenario, belligerents would have to take into account the ongoing adverse impact on the health and welfare of the civilian population resulting from long-lasting environmental damage suffered by the soil and the water as a result of the oil spill. This is supported by State Practice and doctrine: as noted by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia, ‘even when targeting admittedly legitimate military objectives, there is a need to avoid excessive long-term damage to the economic infrastructure and natural environment with a consequential adverse effect on the civilian population.’[[544]](#footnote-544) The assessment of temporally remote events, however, must always be causally linked to the cyber-attack that originated them. In this regard, Richmond has advanced the idea that collateral damage in cyber should also include the possible use, by third parties, of cyber-weapons, which, once deployed against a computer network, are available to a wider range of potentially ill-intentioned users.[[545]](#footnote-545) To take a practical example, consider a situation similar to that of Stuxnet, whose source code was released online some months after the knowledge of the attack became public. [[546]](#footnote-546) If we apply Richmond’s approach to this scenario, we can argue that who launched the cyber-attack should take into account not only the actual damage of the attack, but also any incidental damage that might result if, and only if, a third-party user launches a cyber-attack that relies on Stuxnet source code. Clearly, this interpretation leads to paradoxical results, because the likelihood that a third party user could use a certain cyber-weapon if it will become available to the public cannot be foreseen with sufficient accuracy, not to mention that the quantification of the collateral damage itself will be practically impossible.[[547]](#footnote-547)

### 1.5. The material scope of ‘expected’ incidental harm in the cyber domain.

The first prong of the proportionality analysis defines collateral damage as the ‘incidental loss of life, injury to civilians, damage to civilian objects, or a combination thereof’ that can be expectedfrom an attack. In the cyber-context it is therefore necessary to distinguish between two categories of cyber-attacks, those causing physical violence and those which do not.

The first category does not pose any peculiar issue, as the interpretation of what has been considered as physical damage is relatively flexible and, therefore, easily applicable. Consider again the case of the Stuxnet worm which targeted the Iranian nuclear enrichment plant of Natanz over a nine months period starting from April 2011, damaging several hundreds of turbines.[[548]](#footnote-548) Applying the principle of proportionality to the Stuxnet attack leads to the conclusion that, had it happened during an armed conflict, the attack would have been lawful in principle, since it was directed against a military objective. However, the military advantage gained from the operation (halting or stopping the enrichment of uranium by the Islamic Republic of Iran) would have to be weighed against the incidental ‘damage to objects’ resulting from the attack. If the application by analogy of the principle of proportionality to cyber-attacks causing *physical* violencehas proven uncontroversial, the same cannot be said when it comes to applying proportionality to cyber-attacks that result in effects which are different from physical violence, yet are worthy of regulation by the law of armed conflict.

When it comes to psychological harm, the *Tallinn Manual* has adopted a very narrow approach, stating that effects such as inconvenience, irritation, stress or fear do not suffice to qualify an operation as an attack, because they do not amount to physical violence, and consequently must not be considered within the notion of collateral damage.[[549]](#footnote-549) At the same time, it can be deduced from the commentary accompanying the definition of ‘cyber-attack’ in Rule 30, that ‘severe mental suffering tantamount to injury’ has to be considered in the proportionality analysis as a subset of ‘injury to civilians’. The position taken by the *Tallinn Manual* places a high threshold over what may constitute psychological violence, the assessment of which would therefore be relevant only in very limited scenarios.[[550]](#footnote-550) Despite this interpretation has the benefit of being easily applicable in a battlefield scenario, it appears to be too restrictive. Certainly, it is safe to argue that psychological harm of a modest entity, such as inconvenience or irritation, should not be considered as collateral damage, since it would place too many restraints on behalf of the cyber-attacker. However, the exclusion of symptoms like stress or fear appears problematic, given that IHL already sanctions the launching of attacks the primary purpose of which is the infliction of terror against the civilian population;[[551]](#footnote-551) and while terror is a state of mind more intense then inconvenience or irritation, it does not reach the threshold of ‘severe mental suffering tantamount to injury’, but, rather, appears to be more similar to a state of severe fear. Secondly, even if State Practice has remained silent on the issue,[[552]](#footnote-552) doctrine and jurisprudence have been giving increasing recognition to the idea that adverse psychological effects must be taken into account by the rules of proportionality.[[553]](#footnote-553) In this regard, the most fitting example is the case of *Prlic* before the ICTY. The facts of the case revolved around the destruction, by the Bosnian Croat Military forces (hereinafter ‘HVO’) of the Old Bridge of the city of Mostar in November 1993. The Trial Chamber stated that the destruction of the bridge was within the material scope of Art. 3(b) of the ICTY Statute, which punishes the ‘wanton destruction of town, villages, or devastation not justified by military necessity’[[554]](#footnote-554); in doing so, the Court recognized that the Old Bridge of Mostar was, in principle, a military objective that could have been lawfully targeted, but its destruction was considered to be excessive in comparison to the military advantage gained from the attack.[[555]](#footnote-555) For the purposes of the present analysis, the ICTY reasoning in the *Prlic* case is interesting because it did not stop to an assessment of the physical effects stemming from the bombardment of the bridge, but it went further, highlighting also the symbolic value of the Old Bridge and, as a consequence, the psychological impact that its destruction had against the civilian population.[[556]](#footnote-556) What the Court endorsed in *Prlic* is, in other words, an approach to collateral damage which accounts for a lower threshold of psychological harm as compared to ‘severe mental suffering tantamount to injury’. As a matter of principle, it can be argued that psychological harm can be included within the proportionality analysis in conventional warfare, and the same consideration also applies to the cyber context. This in turn could lead to an increased degree of regulation for cyber-attacks which is consistent with the overarching goal of protecting the civilian population from adverse effects arising from an armed conflict, including those of a serious psychological nature. Having said that, I do believe that the situations in which serious psychological harm can be factored in the proportionality equation are very limited. In Chapter 2 I have argued that ransomware attack like NotPetya and WannaCry are paradigmatic examples of cyber-attacks that are likely to cause serious psychological harm against the civilian population. Yet, these are attacks that are likely to be directed against the civilian population, and not against lawful military objectives, so they are unlawful *per se* and no proportionality calculation does ever occur. In practice, I believe that serious psychological harm can only result from highly destructive cyber-attacks that, at the time of writing, are yet to happen. For instance, a cyber-attack that shuts down the electrical power grid of a region (think something like BlackEnergy, but on a higher scale and for a greater amount of time) or a cyber-attack that disrupts internet access on a nation-wide scale are two instances where symptoms such as mass and severe anxiety should be taken into account in the quantification of collateral damage.

An expansive interpretation can also be advanced in relation to other, non-tangible effects of cyber-attacks, which can be grouped under the label of ‘disruptive effects’. Those are the effects that fall below the threshold of physical violence to individuals and objects, such as economic harm or deprivation of basic services to the civilian population. The approach taken by the *Tallinn Manual* is tailored to the consideration that only physical violence must be accounted for in the computation of cyber collateral damage, leading to the exclusion of economic harm and many forms of disruption, in line with the position expressed by the US Department of Defence in the *Law of War* *Manual*, which considers these kinds of harm too remote.[[557]](#footnote-557) The only exception made by the Commentary is, predictably, the case in which a cyber-attack is expected to cause disruption of functionality of an object, but only if ‘physical replacement of the component’ of the affected network is required.[[558]](#footnote-558)

As already discussed *supra*, this approach is unduly restrictive, and can lead to unreasonable practical outcomes. There may be, for instance, a situation in which a belligerent disables a network that is used both by the opposing party and the civilian population, resulting in the disruption of functionality of a small number of civilian computers and in their physical replacement. In such a scenario, the collateral damage suffered by the civilian population falls under the rubric of ‘damage to objects’ and it is of a very modest quantity when compared to the military advantage gained from disabling the network. Yet, no economic harm would be taken into consideration, even if it could easily outweigh the physical damage caused by the cyber-attack. This paradox becomes even more evident in the case of high-scale disruptive cyber-operations, such as the Shamoon cyber-attacks or those that targeted Bahrein owned companies in August 2018. Leaving aside the question as to whether or not the two targets can qualify as military objectives,

Consider a situation similar to the Shamoon attacks, which targeted the state-owned oil company Saudi Aramco in August 2012, wiping out the data stored in more than 30,000 computers, requiring more than ten days to put them back to operations, and causing an estimated damage of hundreds of millions of dollars,[[559]](#footnote-559) in what has been recognized as ‘the most destructive attack that the private sector has seen to date.’[[560]](#footnote-560) It would seem unreasonable to conclude that no proportionality analysis would have been required on behalf of the attacking party as far as economic losses are concerned. Similarly, the proportionality test should also take into account other disruptive effects affecting the civilian population, such as the interruption of services that are of essential importance for the functioning of a modern society, independently of whether or not their interruption may result in *physical violence*. In this regard, recall that in 2015 a cyber-attack labelled ‘Black-Energy 1’ targeted three energy distribution companies based in Ukraine. As a result, the attack disabled the western part of the Ukrainian power grid, leaving more than 200,000 people without electricity for as long as six hours.[[561]](#footnote-561) Considering that this attack took place in the course of the ongoing armed conflict between Ukraine and Russia, the perpetrators, who were allegedly sponsored by Russia,[[562]](#footnote-562) should have taken into account the disruptive effects which are connected with a power outage, such as the inability to use heating systems and any service which uses electricity to operate. In this regard, it is worth noting that several States have already endorsed a more expansive approach with regards to disruptive, non-physically violent consequences caused by military operations in the context of ‘traditional’ warfare. As such, Norway has expressed the view that ‘military commanders should take into account the humanitarian consequences caused by the attack […] and the more long-term humanitarian problems.’[[563]](#footnote-563) An even broader view has been taken by the UK Inquiry on the intervention against Iraq in 2003, which noted that it is the responsibility of a State ‘to make every reasonable effort to identify and understand the likely and actual effects of its military actions on civilians. That will include not only direct civilian casualties, but also the indirect costs on civilians arising from worsening social, economic and health conditions’.[[564]](#footnote-564)Much like to what has been argued with regards to psychological harm, the inclusion of economic harm and disruptive effects among the reverberating effects falling within the scope of collateral damage is clearly beneficial for IHL as a whole, given that its objective is the minimization of civilian suffering. Furthermore, it better addresses the characteristics of the reverberating effects produced by cyber-attacks.

## 2. Military Advantage.

As opposed to the concept of ‘incidental harm’, the notion of ‘military advantage’ does not pose any unique issue when applied to cyberwarfare. In this regard, the proportionality principles require that the expected collateral damage must be compared with the *direct* and *concrete* military advantage *anticipated* from the attack. Therefore, similarly to what is required for the concept of collateral damage, the military commander must make an aprioristic evaluation of the military advantage, and not an ex post facto determination. Secondly, the words ‘concrete’ and ‘direct’ must be distinguished with how the term is qualified in Art. 48 of AP I, which defines the notion of military objective as an object that ‘by nature, use, purpose or location offers an effective contribution of military action and whose destruction, capture or neutralization offers a *definite* military advantage.[[565]](#footnote-565) Practically speaking, the rules of proportionality have a higher threshold and impose stricter causal and temporal restraints on the attacker when incidental damage is expected.[[566]](#footnote-566) As such, the term ‘concrete’ has been interpreted as requiring the existence of a ‘real’ (i.e., a tangible or measurable) effect, while ‘direct’ relates to the chain of causation between the attack and the military advantage, which must happen ‘without intervening condition of agency’.[[567]](#footnote-567) Furthermore, it must be pointed out that it is commonly understood that *concrete* and *direct* military advantage must be assessed from the attack ‘as a whole’,[[568]](#footnote-568) rather than from isolated or particular parts of the attack. This has important implications in the cyber context, because often cyber-attacks are parts of wider military operations. In this regard, consider a situation like the cyber-attack carried out by Israel in 2007, which switched off the radar systems of Syria with the aim of facilitating the bombing of a nuclear reactor; as such, the concrete and direct military advantage derived from the cyber-attack must be assessed together with the kinetic attack that followed it.[[569]](#footnote-569) Secondly, since a cyber-attack may be directed against multiple computer networks, it would be too restrictive to evaluate the military advantage gained by incapacitating or disabling every single computer network, given that it would be of a very modest entity when taken in isolation; instead, the military advantage gained should be evaluated on the basis of the attack as a whole. In addition to this, the qualification of military advantage as *concrete*  and *direct* stands in opposition to military advantages based on pure speculation: as such, ‘advantages that are vague, hypothetical, indirect, long-term, including possible military advantages that might indirectly derive from advantages in the political, economic, moral or financial realms are therefore excluded’ from the proportionality analysis.[[570]](#footnote-570) The rationale of this distinction is partly practical, partly based on reasons grounded in respect for human dignity. First of all, military advantages which are not concrete and direct but speculative cannot be precisely quantified. Secondly, if the attacking party could factor-in intangible concept such as the need to prevail over the enemy, the notion of military advantage would be conflated in comparison to the expected collateral damage, leading to a more relaxed application of the principle of proportionality, which would be detrimental for the protection of the civilian population. Finally, it is worth discussing whether the concept of military advantage includes force protection, that is, the minimization by the attacking party to the risk to its own soldiers’ safety, and the implications in the cyber context. In this regard, the ICRC has stated that ‘military advantage can only consist in ground gained and in annihilating or weakening the enemy forces.’[[571]](#footnote-571) On the opposite side, some States have adopted a broader view on the matter. For instance, the US *Law of War Manual* notes that ‘military advantage of an attack may involve a variety of […] considerations, including improving the security of the attacking force’[[572]](#footnote-572), a definition repeated with almost identical language in Canada’s *Joint Doctrine Manual*, and in declarations made by Australia and New Zealand in the drafting process of Additional Protocol I.[[573]](#footnote-573) Furthermore, the government of Israel also recognizes that military advantage ‘might reasonably include not only the need to neutralize the adversary weapons and ammunition and dismantle military or terrorist infrastructure, but also – as a relevant but not overriding consideration – protecting the security of the commander’s own forces.’[[574]](#footnote-574) Similar views are also shared by the doctrine: Yoram Dinstein notes that ‘force protection is a valid concern in determining the military advantage of an attack’,[[575]](#footnote-575) while Michael Schmitt has argued that ‘an attack in which the personnel or military equipment are lost is evidently not as self-advantageous as one in which they survive to fight again.’[[576]](#footnote-576) While it can be argued that the concept of force protection also applies to proportionality assessments in cyber warfare, several scholars have, however, advocated for a more cautious approach, highlighting the risk that the inclusion of force protection ‘would blur and decisively undermine the proportionality analysis’,[[577]](#footnote-577) because minimizing the losses of the attacker could justify ‘more and more collateral damages under civilians’.[[578]](#footnote-578) For this reason, they claim that ‘military casualties incurred by the attacking side are not a part of the [proportionality] equation.’[[579]](#footnote-579) These are legitimate concerns, however, it should be noted that force protection must amount to a *direct and concrete* military advantage in order to be counted in the proportionality assessment. In other words, force protection becomes a relevant legal factor only in limited scenarios. An attack may be employed to save one’s own forces from an imminent attack by an enemy: suppose, for instance, that a belligerent has valuable information that an attack against its ground troops will be launched within hours; he then decides to launch a CNA aimed at disabling, or interfering with, the targeting system of the enemy’s fighter jets in an attempt to protect its troops. In this circumstance, the military advantage gained would be sufficiently real and tangible, and causally connected with the attack, to qualify as *concrete and direct*. A similar conclusion may be reached under a slightly different situation, one in which the attack would serve the purpose of destroying the enemy forces to prevent further losses to the attacker’s troops; such is the case of a cyber-attack that causes a malfunction in the energy distribution system of a military barrack located in a residential area, in order to generate an explosion aimed at killing, or incapacitating, the highest number of combatants stationed there and prevent the enemy from launching an attack against its own forces.

In both of the situations depicted above, the value of the military advantage gained from force protection ‘is the value of the forces that are directly and concretely being protected by the threat’ posed by the enemy.[[580]](#footnote-580) In this regard, it is essential to point out that ‘force protection’ must not be confused with ‘the abstract protectiveness of the *means and methods of warfare* used to attack.’ [[581]](#footnote-581) The focus, instead, must always be on the forces that are actually and verifiably being protected, since only in that case it is possible to determine a military advantage which is sufficiently direct and concrete for the purposes of the proportionality evaluation. For this reason, it must be excluded that ‘the remote character of cyber operations, and thus the enhanced security for the attacker, would increase the military advantage they provide and thus would justify a higher amount of collateral damage of civilians and civilian objects.’[[582]](#footnote-582) This approach, as noted by Roscini, is far too broad, because it considers as a military advantage the use of cyber means of warfare as an alternative to other *hypothetical* courses of military action that have not been chosen; as such, launching a cyber-attack will always be safer than any other attack in terms of force protection, and therefore will always yield a military advantage, giving the belligerent the possibility to bypass the limits imposed by the principle of proportionality. However, as argued *supra*, speculative military advantages are not counted within the proportionality assessment.

Most importantly, the military advantage itself does not originate from the cyber-attack, but from the decision not to attack with a different method, such as a ground attack or low-altitude bombing. Therefore, there is no *direct* military advantage that connects the cyber-attack with the protection of one’s own forces;[[583]](#footnote-583) if a causal link does exist, instead, it originates from the decision not to attack with a more unsafe option, which precedes the launching of the actual CNA.

In light of the above considerations, it can be submitted that force protection, as a factor that has to be accounted for in the determination of military advantage, can be applied to cyber-attacks under certain, limited situations. Having said that, the inclusion of force protection ‘has the major disadvantage of introducing a further subjective element in the calculation of proportionality’,[[584]](#footnote-584) as the value of military personnel and material would have to be measured against the expected collateral damage. In this regard, the US Counterinsurgency Field Manual seems to implicitly recognize a hierarchy of values, stating that combatants must ‘assume additional risk to minimize potential harm’ to civilians.[[585]](#footnote-585) Beyond this, however, there is no evidence of State Practice or doctrinal consensus in relation to this specific question.

## 3. Comparing collateral damage and military advantage in cyberspace: the meaning of the word ‘excessive’.

Art. 51 (5) (b) considers an attack disproportionate when the *expected* collateral damage is *excessive* in comparison to the direct and concrete military advantage anticipated from the operation. This is the core of the ‘proportionality analysis’ and the most problematic part, as there is no accurate standard to measure ‘excessiveness’. At the very least, the term ‘*excessive’* is not a synonym with ‘*extensive*’. In other words, a cyber-attack against a military objective does not violate the principle of proportionality for the mere fact that it is expected to cause a large number of civilian casualties; it may very well be an attack directed against a dual-use infrastructure belonging to the opposite party, the destruction of which would cause a *concrete* and *direct* military advantage that could far outweigh the expected civilian casualties and destruction caused to the neighbouring area. At the same time, a cyber-attack expected to cause a modest amount of incidental damage could be disproportionate because it does not provide any significant *concrete* and *direct* military advantage.

With regards to the interpretation of the term ‘excessive’, it requires the ‘reasonable military commander’ to compare incidental harm and military advantage, two values which, as discussed in the paragraphs above, are difficult to quantify, let alone measure against each other. The issue related to the incommensurability of the two values has been acknowledged by the doctrine[[586]](#footnote-586), which has proposed different models.[[587]](#footnote-587) In this regard, it is not within the scope of the present Chapter to discuss them, given that, at the current time, there is no State practice that validates *any* standard.[[588]](#footnote-588) Rather, what seems to be the consensus is that it is not objectively possible to quantify the factors involved in the proportionality assessment,[[589]](#footnote-589) not only because collateral damage and military advantage cannot be estimated with absolute accuracy, but most importantly given that, as Dinstein put it, ‘there is little prospect of agreement between the opposing Belligerent Parties as to the rival values of military advantage and collateral damage’.[[590]](#footnote-590) Instead, it can be argued that the opposing parties are likely to evaluate the components of the proportionality equation in a way that matches their subjective perspective on the battlefield; as such, the attacking party is likely to attribute to military advantage a greater weight than collateral damage, while the defending party’s estimation of military advantage may be different.[[591]](#footnote-591)

In this context, cyber warfare is no different: the problems that are present in the evaluation of what is *excessive* collateral damage may be exacerbated in cyberspace, given the prevalence of dual-use objects, the higher degree of connectivity between civilian and military networks, and the consequent need to evaluate reverberating effects of different nature (physical, disruptive, economic) into the calculation of collateral damage. However, it can be argued that under certain circumstances the comparison between expected collateral damage and military advantage could be less controversial than under more traditional scenarios, considering that cyber-attacks can result in less physical destruction when compared to conventional attacks. As such, the choice to launch a cyber-attack to temporarily shut down the SCADA system of a power plant (consider something similar to Stuxnet) can be expected to cause an amount of death or injury to civilian, or damage to civilian objects, which is inferior compared to a kinetic attack that aims to physically destroy the power plant. Certainly, the military advantage gained from this hypothetical cyber-attack would also be of a more modest entity, since the operating system can be simply materially replaced or put back online. However, should the attacking party decide to user a cyber-attack rather than a kinetic attack, it might expect a lower level of collateral damage. As will be discussed *infra*,[[592]](#footnote-592) this has important implications, considering that there exists an obligation to ‘take all feasible precautions in the choice of means and methods of warfare with a view to avoiding, and in any event to minimizing, incidental loss of life, injury to civilians and damage to civilian objects.’[[593]](#footnote-593) On the other end of the spectrum, there will be also situations in which cyber-attacks can be expected to cause high amounts of collateral damage to civilians and civilian objects, especially when dual-use objects are targeted. In this case, evaluating ‘excessiveness’ will depend on the kind of harm caused by the CNA. In this regard, I submit that not all type of damage should be weighed equally when determining excessiveness.[[594]](#footnote-594) In fact, expected civilian deaths should be valued more than physical injury, and destruction of especially protected objects, such as those indispensable for the survival of the civilian population, need to be taken in greater consideration than the destruction of objects which do not benefit from such protection. Following this line of reasoning, it can then be argued that a cyber-attack that is expected to cause psychological harm, economic harm and other disruptive effects should be (as a general rule) considered as resulting in a lower amount of collateral damage than an attack that is expected to cause physical violence. Compare, for instance, a cyber-attack that is aimed at temporarily disabling the power grid of a small urban area *vis-à-vis* one that will affect an entire city or region: while both targets can be considered as Critical National Infrastructure, the latter will likely generate a higher amount of collateral damage when compared to the former. However, this does not mean that a lower level of collateral damage automatically translates in a cyber-attack that is not ‘excessive’: rather, the very fact that cyber-attacks against dual-use targets can affect a large part of the civilian population by spreading through civilian networks would inevitably conflate the sum total of incidental harm that has to be accounted for in the proportionality equation, even when the damage takes the form of disruption to civilian services, or economic harm.

## 4. Conclusion.

The Chapter has discussed the issues related to the application of the principle of proportionality in cyber-warfare. First of all, it has argued for an expansive interpretation of the notion of ‘incidental harm’, which must consider reverberating effects of cyber-attacks in the form of physical violence (death or injury to civilians, damage of objects) as well as psychological harm, economic harm, and disruption of public services. As such, the Chapter has claimed that the adoption of a wider approach to the concept of ‘incidental harm’ can serve the purpose of ensuring a greater degree of protection to the civilian population against the unique effects of cyber weapons. Secondly, the Chapter has analysed how the concept of military advantage should be understood in the cyber context, claiming cyber-attacks may, only in limited scenarios, be used for the purposes of force protection, thereby increasing the anticipated military advantage and, therefore, allowing for a higher amount of incidental harm. Finally, Section III has discussed the comparison between the two elements of the proportionality analysis. In this regard, while the two concepts of incidental harm and military advantage cannot be measured against each other with sufficient certainty, I have argued that the evaluation of what is ‘excessive’ is facilitated by the very existence of cyber technologies as the possible weapon of choice for attacking a military objective, because cyber-attacks would result in a total amount of expected collateral damage which is inferior to that caused by conventional means of warfare (such as kinetic weapons). Thus, the lower the expected collateral damage caused by a cyber-attack, the higher the possibility that the attack would comply with the proportionality principle. Whether or not this will lead to an increased protection of the civilian population would hinge on the decision to use a cyber-attack *in lieu* of other means of attack, a decision that must be made in accordance with the rules on precaution in attack, which I will critically examine in the next Chapter.

# Chapter 6. The application of the principle of precaution in the cyber domain.

The previous chapters have highlighted how the emergence of cyber-warfare impacts upon the underlying principles of military necessity and humanity, which represent the foundation on which the normative architecture of the *jus in bello* is build. Thus, Chapter 3 has shown how the mere existence of cyberspace changes the meaning of what constitutes a military objective for the purposes of Art. 51 AP I: computer systems and network, nodes and cable of communications and other kind of cyberinfrastructure may be lawfully targeted if they make an ‘effective contribution to military action’ by nature, use, location of purpose and if their ‘destruction, capture or neutralization’ offer a ‘definite military advantage’.

This factor has profound implications for the conduct of hostilities in the cyber context, since it expands the scope of what can be lawfully targeted, either by kinetic or cybernetic means, thereby potentially increasing the total amount of violence against military objectives in cyberspace. Thus, the purpose of this Chapter is to discuss to what extent the rules on precaution under Additional Protocol I can be applied to cyber-attacks, and whether they can be interpreted in order to humanize the conduct of hostilities in the cyber domain. As such, the Chapter consists of three Sections. Section I discusses the issues related to taking precautions in attack. Section II analyses the relevance of precautions against the effects of attacks in cyberspace, and Section III concludes.

## 1. Precautions in attack.

The rules on precaution can be seen as the logical outgrowth of the principle of distinction, along with the principle of proportionality. If, in fact, the latter prohibits direct attacks against civilian and civilian objects and the former places a limit on what can be considered as lawful collateral damage, the principle of precaution requires belligerents to comply with a series of obligations aimed, essentially, at reducing the adverse impact that lawful attacks may have against the civilian population and civilian objects.
The principle of precaution can be dissected into two different branches: precautions in attack and precautions against the effects of attacks.
With regards to the former, Art. 57 of Additional Protocol I provides that ‘in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects’.[[595]](#footnote-595) In order to give effect to this general rule, the provision imposes the following obligations upon ‘those who decide upon or plan an attack’:[[596]](#footnote-596)

1) Do everything feasible to verify that the objectives to be attacked are military objectives.[[597]](#footnote-597)

2) Take all feasible precautions in the choice of means and methods of warfare in order to minimize the impact of attacks on the civilian population.[[598]](#footnote-598)

3) Refrain from launching an attack that might be expected to cause excessive collateral damage.[[599]](#footnote-599)

4) Do everything feasible to cancel or suspend an attack if it becomes apparent that it would violate the principles of distinction and proportionality.[[600]](#footnote-600)

5) Give effective advance warning to civilians prior to an attack.[[601]](#footnote-601)

6) Where a choice is possible between different military objectives, choose the one the attack against which would cause the least damage to civilians and civilian objects.[[602]](#footnote-602)

Before discussing how these rules apply to the cyber domain, it is worth noting that the standard of constant care imposes an obligation of conduct aimed at risk mitigation and harm prevention by the military commander.[[603]](#footnote-603)

Most importantly, the standard applies to the wider category of ‘military operations’, while the rules on precaution under Art. 57 (2) AP I are only concerned with ‘attacks’. In the cyber context, military operations not amounting to attack could be information gathering operations carried out by cyber means, whereas the notion of ‘cyber-attack’, as explained in Chapter 2, can be interpreted in different ways. The Tallinn Manual considers cyber-attacks only those operation which cause *violent effects*, so that they must result in physical damage to individual and objects; any other cyber operation, including those that result in economic damage, or target a critical infrastructure without causing physical damage, would be subject only to the obligation to take constant care, which, in the cyber context, would require a commander ‘to maintain situational awareness at all times, including all phases of the [cyber] operation.’[[604]](#footnote-604) The obligation to take constant care, however, appears to be far less stringent when compared to rules on precaution, as it will be shown in the following paragraphs: considering this, it can be argued that the *Tallinn Manual*’s approach is too restrictive and allows belligerents too much freedom of action in the cyber battlefield. *Vice versa*, in Chapter 2 I have advocated for a more expansive interpretation that extends, also, to cyber-operations causing severe mental suffering, severe economic harm, severe deprivation of essential services, or any effect that adversely impact the dignity of the civilian population on a serious level. Consequently, the list of cyber-operations falling under the scope of the rules on precaution is significantly wider that those listed under the *Tallinn Manual*, thereby increasing the protective scope of the rules to the advantage of the civilian population.

### 1.1. Verification of military objectives.

The obligation of verification is found it Art 57 (2) (a) (i) AP I, according to which military commanders must do ‘everything *feasible*’ to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives. The *rationale* of the rule quite straightforward, as it is aimed to ensure that belligerents would not mistakenly target civilians or civilian objects as military objectives: it represents, therefore, an additional limit to the principle of military necessity in favour of humanity-driven consideration. The focus of the provision lies the notion of *feasibility*, whichoperates as an objective standard found in several of the rules on precautions in attack. In this regard, the meaning of what is ‘feasible’ is to be interpreted as ‘that which is practicable or practically possible’, as shown by the *travaux preparatoires* of the Protocols.[[605]](#footnote-605) A similar view is shared by the US Department of Defense *Law of War Manual*, according to which ‘the standard for what precautions must be taken is one of due regard or diligence, not an absolute requirement to do everything possible.’[[606]](#footnote-606) Therefore, the concept of feasibility must take into account ‘all the circumstances ruling at the time’.[[607]](#footnote-607) This includes factors of humanitarian and military nature, such as the quantity and quality of resources and technology available to the attacker as well as the risk to the attacking forces. What just said does not extend, however, to financial consideration, as ‘there is no basis in international humanitarian law for factoring expense into feasibility assessments’;[[608]](#footnote-608) would that be the case, a belligerent may well invoke abstract and remote economic motives in the feasibility equation as a way to circumvent the obligation to take precautions. Within the concept of feasibility under Art. 57 (2) (a) (i) API, the essential point revolves around how to determine what amounts to ‘practical’, that is, what is the minimum level of information that is necessary in order to verify if a target is civilian or a military objective.[[609]](#footnote-609) In this regard, the military commander it required to take a decision based on the *‘*relevant information available at the time and which it has been possible to obtain to that effect’[[610]](#footnote-610). As such, the rule does not require absolute certainty, but instead poses an obligation on those who plan or decide upon an attack to come to a ‘reasonable belief about whether the object meets the criteria for being a military objective.’[[611]](#footnote-611)This means, *in concreto*, that the specific amount of information necessary to verify the nature of a target is inevitably context-dependent, although, as a minimum, a military commander must ‘must set up an effective intelligence gathering system to collect and evaluate information concerning potential targets’ and employ ‘available technical means to properly identify targets during operations’.[[612]](#footnote-612) Having said that, it must be pointed out that in conventional warfare military commanders are often forced to decide under urgent and difficult circumstances: therefore, there might be situations in which a targeting decision can be made using information that is insufficient to completely dissipate doubts as to the civilian or military character of an object.[[613]](#footnote-613) For instance, an intelligence report might indicate that a civilian building had been used, two weeks prior to the commencement of the armed conflict, as a munition deposit.[[614]](#footnote-614) If the target is attacked and it is later revealed that it is, indeed, a civilian object, that does not necessarily mean that that those responsible for ordering the attack did not comply with the obligation under Art. 57 (1) AP I; rather, what counts is that ‘a reasonable effort’ to obtain relevant information was made and that the military commander believed, in the circumstances ruling at the time, that the target of the attack was a military objective.[[615]](#footnote-615) On the other hand, there might also be cases in which targeting a military objective could potentially lead to a great amount of collateral damage, in which case ‘there should be an increase in the level of caution employed when endeavouring to identify the target.’[[616]](#footnote-616) Therefore, it can be argued that ‘the level of verification required to reduce doubt, and the degree of acceptable doubt, will vary depending upon the likely adverse consequences of a wrong decision.’[[617]](#footnote-617) The above considerations apply also to the cyber context, albeit there exist certain inherent features that make the interpretation of the feasibility standard different from traditional scenarios. That is, primarily, because many cyber-infrastructures could very well be used by civilians and the military, therefore there is the increased likelihood that a cyber-attack may target a dual-use object or, worse, it can target a military objective before spreading into a civilian network. Secondly, targeting decision in the cyber domain are likely to be taken outside a field position in the combat zone, by a military commander that will be assisted by a team of dedicated cybersecurity specialist;[[618]](#footnote-618) thus, the geographical distance from the battlefield eliminates both the risks and the sense of urgency associated with traditional intelligence gathering, which can be seen as mitigating factors in traditional armed conflict scenarios. Because of the combination of these two elements, it can be argued that the threshold of what is considered ‘feasible’ in the cyber context should be placed higher than in conventional warfare, in order to ensure effective protection of civilian objects and the civilian population.

Consequently, a military commander should employ specific verification techniques, such as network mapping[[619]](#footnote-619) and footprinting, [[620]](#footnote-620)the purpose of which is to identify ‘the ownership and geographical locations of the targets and related infrastructure where [cyber operations] will be conducted or cyber effects are expected to occur, and to identify the people and entities […] that could be affected by proposed operations’.[[621]](#footnote-621) Then, the evaluation of the information so obtained must be carefully scrutinized, considering also that an adversary may try to conceal military objectives, for instance by spoofing the IP address of a military installation and make it appear associated with a civilian network.[[622]](#footnote-622) That being said, there might be instances when taking precautions in the cyber domain is not feasible, as when a network mapping procedure risks disclosing information that can allow the enemy to defend itself against the incoming cyber-attack: in this case, the military commander should refrain from launching the cyber-attack because there was no verification process as to whether the targeted computer system, network or infrastructure was a civilian object or a military objective. The above situation must be distinguished from when all feasible precautions have been taken to verify the target, but doubt persist as to the nature of the targeted object. According to Art. Art. 52 (3) API, in case of doubt whether an object is a civilian object or a military objective, it shall be presumed to be a civilian object and, therefore, not be made the target of an attack.[[623]](#footnote-623) In this regard, it must be however noted that the military commander may still lawfully decide to launch the proposed cyber-attack against those part of the computer network or system for which there is sufficient information to verify their status as lawful targets.[[624]](#footnote-624)

### 1.2. The obligation of minimizing collateral damage in the choice of means and methods of warfare.

Article 57(2) (a) (ii) AP I provides that military commanders must ‘take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event of minimizing, incidental loss of life, injury to civilians and damage to civilian objects.’

Similarly to Art. 57 (2) (a) (i), the rule in question realizes a compromise between the principle of humanity, embodied in the obligation to avoid and minimize collateral damage, and the principle of military necessity, since the notion of feasibility has the primary function of allowing military commanders to avoid doing something that is not practically possible in the circumstances ruling at the time. With regards to the scope of the application of Art 57 (2) (a) (ii), the primary obligation is that of avoiding any amount of collateral damage to the civilian population and civilian objects; it is only when total avoidance is not feasible that the goal of minimizing incidental damage would come into play.[[625]](#footnote-625) Furthermore, the obligation to avoid and minimize is functionally linked to the principle of proportionality and the prohibition to launch indiscriminate attacks. This means that is not sufficient for an attack to cause collateral damage which is not excessive in relation to the military advantage anticipated, but ‘there is also a positive obligation to reduce the expected collateral damage by taking all feasible precautions.’[[626]](#footnote-626) Therefore, there might be instances where an attack that complies with the proportionality principle might still be subject to legal review in order to ascertain if collateral damage could have been avoided or minimized should feasible precautions were taken.[[627]](#footnote-627)

With regards to the requirement to ‘do everything feasible’, it is analogous to that of taking ‘all feasible precautions’ in the verification of targets, so similar considerations made in subsection 1.1 *above* would apply: the standard is not one of absolute certainty and, as we shall see, it must be interpreted taking into accounts the circumstances ruling at the time.

A contentious point for the cyber domain relates to whether the notion of *feasibility* imposes an obligation to acquire new weapons and information technology, as has been argued by *Human Rights Watch* in its review of the US bombing campaign during the First Gulf War.[[628]](#footnote-628) This position, however, has no bearing in current IHL,[[629]](#footnote-629) and has been rejected, *inter alia*, by several States including the US, who instead argue that ‘there is no specific obligation’ on Belligerent Parties to use modern weapon technology, such as precision guided munitions (PGMs),[[630]](#footnote-630) or even cyber-attacks, because there will be situations in which it will not be *feasible* to do so. In practice, what is *feasible* will have to be determined on a case-by-case basis and will be influenced by several factors, such as the level on which the decision to launch an attack is made, the type of weaponry available in a given situation, the degree of military advantage gained by choosing a specific means of attack (for example, a cyber-attack instead of a kinetic attack) or even the use of a certain method of attack over another, such as the decision to launch an attack against a military target by night, in order to reduce the risk of collateral damage. The lack of a general obligation to always rely upon the most precise or modern weapon means that belligerents are not, *a priori*, compelled to resort to a cyber-attack to avoid or minimize incidental damage. That having being said, the very existence of cyber as a mean of warfare further humanizes the impact of the rule: in fact, there will be circumstances in which belligerents might be required to use cyber-weapons, instead of kinetic weapons, due to the fact that a cyber-attack may target a military objective, and achieve a military advantage, without causing the degree of physical damage that is commonly associated with kinetic means of warfare. [[631]](#footnote-631) This feature of cyber-weapons has been already pointed out by Michael Schmitt, who notes that:

‘Whereas in the past physical destruction may have been necessary to neutralize a target’s contribution to the enemy’s efforts, now it may be possible to simply ‘turn it off’. For instance, rather than bombing an airfield, air traffic control can be interrupted. The same is true of power production and distribution systems, communications, industrial plants, and so forth.’[[632]](#footnote-632)

Considering this, we can argue that the obligation to rely to cyber-attacks as in order to comply with Art. 57 (2) (a) (ii) will arise in two distinct scenarios.

Firstly, if a kinetic attack would yield a greater degree of military advantage compared to a cyber-attack, but it would violate the principle of proportionality, the obligation to avoid and minimize collateral damage becomes relevant, requiring belligerent parties to rely on a cyber-attack to achieve the desired military outcome. Consider a scenario similar to the Stuxnet worm cyber-attack: in this case, the attacker aims at interrupting the production of enriched uranium to prevent the enemy from developing nuclear weapons in the future, so it designates a nuclear powerplant as a military objective. At this point, the military commander must decide what means of attack to employ in order to achieve the desired military outcome. Suppose that he has intelligence informing him that an airstrike against the power plant would kill a great number of civilians and cause damage to the surrounding environment, due to the release of radioactive material following the physical destruction of the target, in a way that he deems excessive in relation to the military advantage anticipated from the attack; as such, the attack, if carried out by kinetic means, would risk violating the principle of proportionality. The target could, however, also be attacked through a cyber-operation, engineered to interfere, undetected, with the functionality of the turbines responsible for the uranium enrichment process and, ultimately, cause them to malfunction and stop operating altogether; in this situation, the destruction of the turbines would be the only physical damage resulting from the attack and would likely not be deemed excessive for the purposes of Art. 51. Certainly, the military advantage gained from launching a kinetic attack would be superior, considering that the nuclear site would be destroyed, instead of being rendered temporarily inoperable, but at the risk of violating the principle of proportionality. Therefore, the choice of relying on a cyber-attack would satisfy the requirement of avoiding or minimizing collateral damage to the civilian population. Clearly, it must be noted that the obligation to avoid or minimize collateral damage would not require the attacker to launch a cyber-attack if the airstrike against the nuclear installation is compliant with the principle of proportionality (since, *ceteris paribus*, it would still result in a greater military advantage if compared to a cyber-attack). Secondly and finally, the obligation comes into play when two means of attack (i.e. kinetic *versus* cyber) or methods of attack (i.e. two different kinds of cyber-attack) would yield the same military advantage, in which case it must be chosen the one which minimizes collateral damage to the civilian population and objects.[[633]](#footnote-633) For instance, if the military advantage sought is to interrupt the provision of electricity to an enemy military base, a cyber-operation that causes the system to shut down by overloading it with requests should be preferred to a cyber-operation that corrupts data, which could spread to civilian networks and system and which could result in physical damage.[[634]](#footnote-634) Further to this point, it must be noted that the obligation to launch a cyber-attack is influenced by the fact that the protection of the attacking forces is factored in the notion of feasibility. As such, a belligerent may consider not feasible to launch an airstrike against a military objective by flying at low altitude, because the increased risk to the safety of the pilot will, presumably, put him in a situation where he will not be complying with the obligation to avoid or minimize lawful collateral damage to civilians. Therefore, if a similar military advantage can be gained by resorting to a cyber-attack, the military commander is required to choose the former over the latter.

### 1.3. Precautions related to the principles of proportionality and distinction.

Art. 57 (2) (b) AP I provides that those who plan and decide upon an attack must ‘refrain from launching any attack which might be expected to cause incidental loss of 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.’ Similarly, Art 57 (2) (b) requires those who plan, decide or *execute* an attack to cancel or suspend said attack if it becomes apparent that it would violate the principle of proportionality or when the target is not a military objective, or is subject to special protection. The *rationale* of both rules is quite intuitive, as they require the attacker to take into account, as a matter of precaution in the phases preceding the launching of an attack, the principles of proportionality and distinction. With regards to the obligation to refrain from launching disproportionate attacks, its application to the cyber domain has already been discussed in Chapter 5, in the context of the principle of proportionality, and no further discussion is needed in the present Chapter. What is more problematic is the obligation to cancel or suspend attacks. One issue revolves around the specific competences necessary to apply the rule, since its addressees are not only military commanders (‘those who plan or decide upon an attack’) but also to those who are executing the attack. To take a practical example, suppose that a soldier has infiltrated within the SCADA system of a power grid which generates electricity used by a military barrack, in order to shut down the provision of electricity to the enemy in that area. It is later discovered that shutting down the power grid will affect a number of civilian infrastructures, including a hospital, so civilian loss of life might be expected. Under this scenario, the soldier will possess the technical competences required to launch the cyber-attack, but he most likely will not have the necessary skills to make a proportionality assessment; as discussed in Chapter 5, evaluating collateral damage in the cyber domain is a notoriously difficult endeavour, because cyber-attacks might result in various kinds of indirect effects against the civilian populations and civilian objects. Considering this, it might be argued that the obligation to suspend or cancel an attack will rest, primarily, upon military commanders and, generally, on those who are ‘higher in the chain of command and possibly, those with a sufficient knowledge of all aspects of the attack to determine that excessive incidental losses will probably be incurred.’[[635]](#footnote-635) Therefore, military commanders should have an obligation to supervise all phases of the cyber-attack, which in practice would require the commander either to have a specific knowledge of the cyber-weapons and the techniques employed in each attack or, more realistically, to be assisted by a team of specialists.

A second question relates to the technical capabilities required to cancel or suspend an incoming cyber-attack. In this regard, Art. 57 (2)(b) AP I applies when ‘it becomes apparent’ that an attack would violate the principle of distinction of proportionality. In conventional warfare, this is limited to situations where the attacker has a visual cue that something is amiss: to put it differently, a pilot may notice, upon firing its weapon to a military objective, that the target is actually a civilian one and, accordingly, refrain from launching the attack. In the cyber context, the practical applicability of the rule seems even more limited, given the virtuality of cyberspace and, most importantly, the fact that a cyber-attack may result in indirect and often delayed effects, depending on the kind of cyber-weapon used. Consider the case of a cyber-attack that consist in employing a malware that will execute a logic bomb within the target computer system, in order to destroy the physical infrastructures operated by said system.[[636]](#footnote-636) Suppose, then, that before the conditions that trigger the activation of the logic bomb are met, it is discovered that the malware would spread to civilian networks. Under this scenario, the ‘execution’ of the cyber-attack begins from the moment in which the cyber-attack is launched (which would be when the malware interacts with the *data* in the target computer system) to the moment in which it results in the desired effects (that is, upon activation of the logic bomb). Therefore, the obligation to cancel or suspend the attack should accordingly cover all steps of the execution phase, requiring military commanders and attackers to monitor the cyber-attack as it unfolds and, furthermore, retain control of the cyber-attack after its initial deployment against the target system, in order to cancel or suspend it if necessary. That having been said, there would be situations in which cancelling or suspending a cyber-attack will not be considered *feasible* (as in ‘practically possible’), such as when the cyber-weapon of choice is a computer worm, which is designed to act autonomously (that is, without human intervention). Clearly, in a similar scenario, the rule will cease to apply once the payload has been deployed by the code, and any collateral damage the cyber-attack may result in would have to be factored in the proportionality assessment under Art. 51 AP I.

### 1.4. The obligation to give effective advance warning.According to Art. 57 (2) (c) AP I, ‘effective advance warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit.’[[637]](#footnote-637)

The rule is intended to limit the impact of attacks against the civilian population, and has been applied on several occasion in conventional scenarios: for instance, the Israeli Defense Force (IDF), during the Israel-Lebanon war of 2006, developed the practice of giving warnings by dropping leaflets in the areas surrounding the targets, make radio announcements or sending text messages to civilian phones minutes prior to the execution of an attack.[[638]](#footnote-638) The provision is comprised of two parts. Firstly, it requires to give ‘effective advance warning’ but only with regards to ‘attacks which may affect the civilian population.’ Thus, the wording of the rule implicates that in certain circumstances the obligation to issue a warning would not arise, such as when the attacker launches a cyber-attack against a military objective which is secluded from the civilian populations and from civilian buildings. However, in the cyber domain the obligation would come into play in many situations, considering that present-day hostilities often take place in urban areas, and that there exists a very high degree of interconnectivity between civilian and military infrastructures. With regards to the requirement that the warning must be ‘effective’, a relevant question revolves around the level of what the level of detail for a warning is to be considered effective. Generally speaking, the obligation is subject to stringent conditions. Thus, according to the UK Military Manual:

‘The object of a warming is to enable civilians to take shelter or leave the area and to enable civil defence authorities to take appropriate measures. To be effective the warning must be in time and sufficiently specific and comprehensive to enable them to do this.’[[639]](#footnote-639)

The effectiveness of the warning must also be evaluated in the circumstances of each case, and according to different factors, such as the ability of the civilian population to understand its meaning or to act upon it. [[640]](#footnote-640) Moreover, a warning cannot be considered effective if the instructions given cannot be followed due to the conduct of the attacking party, or if it is not issued within a reasonable time.[[641]](#footnote-641) The above considerations can be easily translated to the cyber domain, where the possibility to issue a warning is made easier by the fact that the message can be delivered through cyberspace with minimal risk to the safety of the attacking forces. Thus, instead of issuing a warning by dropping leaflets from an aircraft, the attacker can choose to inform the civilian population of the upcoming attack (carried out by kinetic or cyber means) through a message sent on a website, via email or SMS. In this regard, it is safe to argue that the use of cyber technology amplifies the humanitarian character of the rule and allows a greater level of compliance with the obligation in question. What just said needs, however, to be counterbalanced with the implications raised by the second part of the provision, according to which the warning must be given ‘unless circumstances do not permit.’[[642]](#footnote-642) The scope of the prohibition has been interpreted to include situations in which the element of secrecy is crucial for the success for the attack or the security of the troops.[[643]](#footnote-643)

In this regard, the success of cyber-attacks is inextricably linked with the fact that they can be covertly deployed against an unaware enemy: thus, the more effective the warning, the more likely it is for the cyber-attack to be deprived of its surprise factor. In light of this consideration, we can argue that the scope of the exception is enhanced in the cyber domain, and the applicability of the obligation to issue an effective warning is more likely to arise in situations where the cyber capabilities of the attacker are superior to those of the defender.[[644]](#footnote-644) In those circumstances, the attacker would not risk the success of the cyber-operations by warning the civilian population that a cyber-attack against a military objective is imminent. Otherwise, in a scenario where the attacker and the defender have equal, or similar, cyber warfare capabilities, issuing an effective warning would allow the defending party to adopt effective defence measures to counter or repel the cyber-attack. Therefore, the attacker could be excused for not complying with the provision, since ‘the specific circumstances of the planned operation do not make it possible to inform the defender because the purpose of the operation could not then be achieved.’[[645]](#footnote-645) To put it practically, suppose that States A decides to target the oil production facilities of State B, which generate fuel which is used by State B’s armed forces. The weapon of choice is a cyber-attack that would result in the explosion of a pipeline and would put at risk the life of the civilian employees working within the facility. The attacking State is under the obligation to provide effective advance warning in order to minimize any incidental damage from the cyber-attack. However, the obligation is only valid insofar as giving the warning does not compromise the success of the cyber-attack. Clearly, this legal outcome is far removed from the objective of protecting the civilian population, and strongly favours considerations related to military necessity. Yet, given its textual limitations, I do not believe that the rule can be applied in a way that enhances human dignity-driven considerations without excessively restricting the freedom of action of belligerent parties.

### 1.5. The obligation to choose the military objective the attack to which causes the least damage among civilians.

According to Art. 57 (3) AP I, ‘when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.’

The rule is comprised of two parts. The first part compels the attacker to evaluate whether targeting different military objectives would result in the same degree of military advantage, that is, a military advantage which is similar but not identical.[[646]](#footnote-646) Despite, as noted by Henderson, the process of ‘calculating military advantage is not exact’,[[647]](#footnote-647) it is possible to envision situations in which the rule might be applicable in the cyber domain. As such, if the objective of the attack is to interrupt electricity distribution to a military installation, the attacker may choose between several options, all of which would yield a similar military advantage. He may target the power generation station as a whole with a kinetic attack; or he might launch a cyber-attack against the distribution network that serves the military site, thereby shutting off the supply to the target system; finally, he may decide to focus on the target system itself, by infiltrating within the network of the military installation and disable an essential component that prevents the system from functioning. Given that the above mentioned methods result in a similar military advantage,[[648]](#footnote-648) the deciding criterion is provided by the second limb of Art 57 (3), which requires, essentially, to make a proportionality evaluation between different military objectives, and choose the one the attack to which would cause the least ‘danger’ to civilian lives and civilian objects. In this regard, the term ‘danger’ has to be interpreted as a synonym of collateral damage, which, in light of what has been discussed in Chapter 5, extends to direct and indirect effects and includes, besides physical violence, psychological violence, economic harm and deprivation of services essential for the civilian population.

This makes the comparison between military advantage and collateral damage especially difficult, and further complicates the determination of what kind of attack among those available results in ‘the least danger’ against civilians and civilian object, since more elements would have to be accounted for within the proportionality assessment. A practical solution to this *dilemma* is to establish a hierarchy of values between different sources of collateral damage, based on their impact on the dignity of the civilian population. Accordingly, it is safe to argue that violence to individuals, in the form of death or injury, should be held in the highest regard, since physical integrity represents the core element of human dignity. Beyond that, physical damage to objects should have a greater weight than psychological damage to individuals in the majority of cases, even if the determination of which attack would result in the least danger will depend on the circumstances of each case. Conversely, a lower value (comparatively) should be assigned to the causation of economic harm. If we apply this reasoning to the scenario where a power generating station is targeted by a cyber-attack, we can conclude that targeting the power generating station with a kinetic attack will, most likely, result in physical damage to objects and, if civilians are near the military objective, incidental loss of life and injury. Furthermore, the attacker should consider indirect effects that may result as a consequence to the interruption of electricity to the surrounding area, such as power outages and fires. Conversely, using a cyber-attack to shut down the operating system of the power grid would cause the least amount of collateral damage, most likely consisting of indirect effects of a physical nature. Therefore, where a choice is possible between several military objectives, which would result in the same military advantage gained, an attack against a cyber-infrastructure should be preferred in the vast majority of cases.

## 2. Precautions against the effects of attacks.

The previous Section has discussed the applicability to the cyber domain of the rules on taking precautions in attack. This Section analyses what precautions must be taken *against the effects of attack*. In this regard, Art. 58 provides the following:

‘The Parties to the conflict shall, to the maximum extent feasible:

(a) without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;

(b) Avoid locating military objectives within or near densely populated areas;

(c) Take the necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.’[[649]](#footnote-649)

Unlike Art 57 which is directed to ‘those who plan or decide upon an attack’, the obligations listed under Art 58 are specifically addressed to the defending party and consist in passive measures to further protect the civilian population and civilian objects from the adverse effects of hostilities. Similarly, to Articles 57 (1) (2) (a) and (b) AP, the precautionary measures are subject to a requirement of feasibility that must be assessed depending on the circumstances ruling at the time. Consider, for instance, a situation in which the defending party has anticipated a kinetic attack against a bridge. The bridge would be considered as a civilian object under normal circumstances but has been recently used by the army as a mean to transport ammunitions and weapons to a nearby military installation. Therefore, it can be argued that it would qualify as a military objective under Art. 52 AP I, considering that it makes an effective contribution to military action, and its destruction would offer a definite military advantage to the attacking party, because the attack would result in an interruption of the enemy’s logistic routes. Pursuant to their obligations under Art. 58, the defending part must, to the maximum extent feasible, endeavour to vacate the civilian population and civilian objects to the vicinity of the target (for instance, by closing the bridge to civilian traffic). Furthermore, it would need to avoid placing the bridge in proximity to densely populated areas, in order to reduce the likelihood that an attack against a lawful target might result in collateral damage. As evidenced, the humanitarian character of the provision cannot be understated; however, despite its status as customary international humanitarian law is well recognized,[[650]](#footnote-650) the actual observance the rule has been very limited.[[651]](#footnote-651) This is due to the fact that the obligations under Art. 58 are weaker than those on the attacker, since failure to comply does not constitute a grave breach of the Geneva Conventions.[[652]](#footnote-652) Furthermore, there seems to be an inherent tension between Art. 58 and the very notion of military objective that hampers the effectiveness of the rule. In other words, while it might be considered feasible to remove the civilian population from the vicinity of a military objective by nature, as well as to build military installations outside of populated area, it is not as feasible to do so when it comes to civilian objects which by their use, location or purpose may be lawfully targeted.

The existence of dual-use objects as a limit to the effective application of Art. 58 AP I is amplified in cyberspace, where there is an unprecedented degree of interconnectivity between the civilian and military sector. [[653]](#footnote-653) This is highly problematic, considering that the scope of application of Art. 58 AP I would include both physical objects (such as cable of communications, hardware components of a computer system) as well as virtual objects (*digital data* stored within a computer, or pieces of code that perform essential functions within the operating system of a civilian infrastructure). As far as physical objects are concerned, the obligation to remove the civilian population is highly context dependent. It would be certainly feasible to do so when a cyber-attack is expected to target the operating system of a dam or a power plant; however, the opposite would be true in the case of a cyber-attack against a node of communication that spreads across a civilian neighbourhood. In relation to the obligation of avoiding locating military objective nearby densely populated areas, that would require the military to build their own communication systems and to separate them from civilian ones, as well as to develop their own hardware and software components. While that would be theoretically possible, as of today there is an increased shift towards civilianization, since the vast majority of governmental communication travel through cables owned and operated by private companies, which are also providers of hardware components to the military sector.

Similar applicative issues emerge with *digital data*, primarily in relation to the obligation to segregate military objectives from densely populated areas. Applied to the immaterial dimension of cyberspace, the obligation would require the defending party to establish a physical airgap between civilians and military operated computer systems and networks, so that any amount of information can travel within the military network, but not outside of it. In this way, if a cyber-attack would target a military computer system in order to corrupt data, it would not spread to civilian networks. Having that said, it would not be feasible to adopt segregation-related measures to certain dual-use objects, such as the Global Positioning System (GPS) or the cyber-infrastructure of a State’s national grid, given their near-universal employment by the civilians and the military.

These shortcomings notwithstanding, the defending party will, however, be able to implement ‘all other necessary precautions’ under Art. 58 (c) AP I. This obligation has a residual character, so it would come into play when a State is not able to comply with paragraphs (a) and (b), thus enhancing the protective scope of the rule. Relevant precautions to be taken in advance against future cyber-attack consist, firstly, in the identification, on behalf of the defending States, of what cyber-capabilities it deems essential to safeguard during an armed conflict and, secondly, in protecting the civilian systems, companies and network that are necessary to maintain the functionality of those cyber-capabilities.[[654]](#footnote-654) Then, the defending State must employ measures of cyber hygiene such as the use of anti-viruses,[[655]](#footnote-655) the execution of data back-up to facilitate data recovery and resumption of service after a cyber-attack,[[656]](#footnote-656) the distribution of protective software and the monitoring of network and systems among others.[[657]](#footnote-657)

## 3. Conclusion.

The above sections have discussed the applicability of the rules on precaution in attack and against the effects of attack in the cyber domain. What has emerged is that cyberwarfare presents unique applicative challenges, due to the fact that the rules on precautions were conceived to address conventional and urban warfare, at a time where cyberspace did not exist. And even if resort to analogy is certainly possible, there is no denying that certain parts of Art. 57 and 58 are almost inapplicable to the cyber domain. Consider, for instance, the obligation to give effective advance warning, the humanitarian potential of which is greatly diminished by the fact that the success of a cyber-attack is linked to its secrecy. Similarly, implementing the obligations of segregation under Art. 58 would require, in practice, massive financial investments by States, in an age where the trend is that of progressive integration between military and civilian systems. Yet, integration comes at the cost of reduce effectiveness of the rule and, thus, a lack of protection from cyber-attacks.

Despite these issues, cyber-weapons also present belligerents with the opportunity to improve the protection of the civilian population and civilian objects. That is the case with regards to the obligation to choose the means and methods of warfare in order to avoid and minimize collateral damage, as well as the obligation to target the military objective the attack on which would result in the least danger. Even if the actual applicability of these rules will arise in limited scenarios, they would nonetheless decrease the sum total of violence in an armed conflict, therefore their humanizing impact cannot be underestimated.

#

# Concluding remarks.

The main focus of my thesis has been the application of a human dignity-oriented interpretation of the rules of targeting to the emerging phenomenon of cyber-warfare, in order to inquire whether the process of humanizing warfare can be further advanced. To pursue this objective, after having provided a definition of what ‘cyberwarfare’ is, I made the claim the process of humanization is the result of the interaction between the normative-ideational principles of military necessity and humanity. Within this process, the scope of application of the principle of military necessity has been progressively reduced and counterbalanced by the emergence of the principle of humanity; this has impacted the law of armed conflict both in the context of norm-creation and in the interpretation of its rules, placing more restrictions on the conduct of hostilities and reducing the total sum of violence experienced in armed conflict.

Chapter 1 inquired as to what makes the principles of military necessity and humanity so different from each other. In this regard, I claimed that the former has a permissive function within IHL, allowing belligerents to employ violence in order to accomplish their military objectives. As opposed to how the principle operates in other areas of international law, namely International Human Rights Law and the *jus ad bellum* regime, where necessity performs a restrictive function, military necessity does not require the existence of a situation whereby recourse to violent measures is a last resort option; rather, military necessity seems to be more akin to military effectiveness.[[658]](#footnote-658) Thus, it is a concept that is inherently expansive, and its unchecked application to the law of armed conflict leads to unrestrained warfare. This is why the principle of humanity exists in opposition to the principle of military necessity; while the former is permissive, the latter is restrictive in nature. In this regard, I chose to define the substance of the principle of humanity as being the idea that the dignity of the individual must be respected and ensured, even in times of armed conflict. Accordingly, I have then explained in what sense human dignity can be construed as ‘foundational’ to IHL and what are its core elements. This required me to trace the path of the evolution of human dignity over time, from its origins within the Stoic philosophers of ancient Rome to its modern meaning, when the concept of human dignity appears to be closely connected, at least on a logical basis, with that of human rights. In this regard, I employed an account of human dignity which has been inspired by James Griffin, who has dissected the concept into the three stages of autonomy, liberty and wellbeing. Each of these tree stages encompasses a series of values that give rise to normative demands that are ensured and protected by a catalogue of human rights both at the national as well as the international level. Yet, I have shown that since the International Human Rights Law regime is of limited applicability in times of armed conflict, it is the task of the principle of humanity to protect the core elements of human dignity to the greatest extent possible. Therefore, the second objective of Chapter 1 has been that of showing how exactly the protection of human dignity is related to and is integrated with the principle of military necessity in the law of targeting, a set of rules of quintessential importance within the normative architecture of IHL, as they regulate the amount of violence that the parties to the conflict may lawfully exchange in the battlefield. An examination of the rules of distinction, proportionality, precaution and unnecessary suffering has shown how the principles of military necessity and the principle of humanity are oppositional in nature, thereby creating a balance which is dynamic, rather than static, and which may shift overtime – for instance by virtue of diverging interpretations over the meaning of certain rules of IHL which were created as a result of the humanization process itself. In this context, the emergence of cyberwarfare raises several challenging questions, the most important one is to define what amounts to an ‘attack’ for the purposes of the *jus in bello*.

The issue has been examined by Chapter 2, in which I have argued how the notion of attack has been anchored to a traditional understanding of violence, a concept which has always been analogized with physical effects (death or injury to individuals and/or damage or destruction to objects). The identification of the notion of ‘attack’ with the concept of physical violence makes sense when applied to kinetic weapons and their ability to adversely affect the dignity of the civilian population, but is problematic when applied to cyber-operations, as I have highlighted by discussing the shortcomings of the interpretation adopted by the Tallinn Manual, the so-called Kinetic Equivalence Effects (KEE) test. Instead, I have argued in favour of a qualitative reinterpretation of the notion of violence in the cyber context, which is focused on the relationship between cyber-operations and the different ways in which they can impair the dignity of the civilian population. I have then proposed the adoption of an expanded definition of what amounts to a cyber-attack which would consist in (beyond cyber-operations causing physical violence) cyber-operations causing serious psychological violence, serious economic violence or a combination thereof. As a result, a wider range of cyber-operations would fall within the meaning of Art. 49 AP I, such as ransomware attacks, identity theft attacks, cyber-operations against Critical National Infrastructures among others. For that reason, subjecting them to the rules of targeting results in a greater degree of protection for the civilian population and for civilian objects and would further improve the humanization process.

The thesis has further examined, in Chapter 3, how cyberwarfare affects the dualism between military necessity and human dignity-driven considerations with regards, first of all, to the distinction between lawful and unlawful combatants. While it is not strictly related to the rules of targeting *per se,* the concept of lawful combatancy is instrumental for the conferral of POW-related rights, and thus closely connected to considerations grounded on respecting the dignity of the combatant. An analysis of the relevant provisions on POW status has shown, however, that recourse by an analogy as an interpretive method is greatly limited by the differences between the cyber context and how hostilities were fought when the Hague and Geneva Conventions were drafted: requirements such as those of ‘wearing a fixed distinctive emblem recognizable at a distance’ and ‘carrying arms openly’ have little practical relevance in cyberspace. The second aspect that I focused on in Chapter 3 has been to discuss how the principle of distinction between civilians and combatants operates in cyberspace, by engaging with the notion of direct participation in hostilities as it has been understood in the ICRC *Interpretative Guidance*. The result of my analysis concluded that the notion of DPH has a greater scope of application in the cyber context than it has in conventional warfare, since the requisite of ‘threshold of harm’ includes, beyond cyber operations that adversely affect the military capacity of the adversary, all cyber-operations which can be qualified as attacks under the definition that I have provided in Chapter 2, which is not limited to the causation of physical violence and includes severe psychological violence, significant economic violence or a combination thereof. Furthermore, I examined the temporal dimension of the concept of DPH (the so-called ‘revolving door’), aligning myself with the expansive approach given by the Tallinn Manual, whereby if a hacker commits separate acts of direct participation he would lose protection from attack for the entire time in which he is engaged in repeated harmful cyber-operations. What are the consequences of applying the principle of distinction in the cyber context, as far as the protection of human dignity in times is concerned? Clearly, the increased scope of application of DPH means that a higher number of individuals can potentially lose their protection against direct attack, which would, therefore, also increase the total amount of violence (either physical or of other types) that combatants can lawfully deploy during hostilities. However, this is a necessary price to pay when the alternative would be that of allowing individual ‘cyber-warriors’ to operate outside the regulatory framework of IHL. I then examined, in Chapter 4, how the distinction between military objectives and civilian objects applies in cyberspace. The most peculiar aspect in this regard revolves around the fact that digital data qualify as ‘objects’ under IHL and can, therefore, considered as military objectives if they meet the cumulative requirements provided by Art. 52 (2) of AP I. Furthermore, and similarly to what I have argued in Chapter 3, I have argued that the mere existence of cyberspace widens the definition of what objects can be lawfully made the object of a kinetic or cyber-attack –especially considering that dual-use cyber infrastructures are predominant. Therefore, this calls into question the application of the principle of proportionality. As such, I have argued in Chapter 5 that the notion of ‘incidental damage’ must be expansively construed, in the sense that it should include, beyond direct effects, also ‘reverberating’ or ‘knock-on’, second and third order effects of cyber-operations qualifying as cyber-attacks. More importantly, these effects are not only limited to the causation of physical violence to individuals or objects; rather, combatants must take into account any serious psychological violence and serious economic violence that may be result from the cyber-attack. In relation to the concept of ‘direct military advantage’, I have claimed that it must be interpreted narrowly, in order to avoid interpretations whereby the use of cyber-attacks can be considered as yielding a greater amount of military advantage when compared to conventional attacks (since a cyber-attack does not pose any risk to the life of the attacking forces, as opposed to a conventional attack), as this would allow combatants to bypass the effectiveness of the proportionality principle. At the same time, when evaluating incidental damage against anticipated military advantage, I have stressed the importance of giving a greater legal weight to the causation of physical violence as a component of collateral damage, rather than serious psychological or economic violence. Finally, Chapter 6 has discussed the application of the principles of active and passive precautions in and against the effects of attacks in the cyber context. It has argued that the rules on precaution can be transposed to the cyber domain only to a somewhat limited extent, since obligations like that of giving effective advance warning or segregating military objectives from civilian objects are likely be ineffective in cyberspace, due to its unique nature. However, a certain *modicum* of humanization can still be achieved by requiring belligerents to choose, under certain specific circumstances, to employ cyber-attacks as a mean to avoid or minimize collateral damage. In conclusion, what is the result of applying a human-dignity oriented interpretation to the rules of targeting, if the aim is that of reducing the adverse effects of cyberwarfare on the civilian population? I believe that the results are only partially satisfying. Clearly, the re-interpretation of the notion of attack that I have outlined in Chapter 2 directly enhances the protection of the civilian population and civilian objects, and undoubtedly has the potential to ‘humanize’ the conduct of hostilities in cyberspace. On the other hand, however, a more expansive definition of attack also means a wider scope of the notion of direct participation in hostilities. This consideration, coupled with the fact that digital data qualify as ‘object’, not to mention the high reliance on dual-use cyber infrastructures that can be qualified as ‘military objectives’, leads to the conclusion that the number of individuals and objects that could be lawfully attacked can be greatly increased. And while the application of the principle of proportionality and precaution can certainly contribute to the objective of achieving a more humane conduct of hostilities in cyberspace, there are certain textual limitations and applicative issues that cannot be circumvented only by means of interpretation. Furthermore, the task of humanizing the law of cyber-targeting does not end with the protection of the civilian population but can also be extended to the protection of combatants in ways that go beyond the conferral of POW status in international armed conflicts. In fact, it is commonly acknowledged that combatants forfeit their protection from attack and can therefore be lawfully targeted and killed, so that marginal attention has been given to safeguarding their dignity, to the exclusion of the above-mentioned POW status and the principle of unnecessary suffering. These considerations are all the more evident in cyberspace, where lawful cyber-combatants and direct participants in cyber-hostilities can be targeted by lethal force (be it the result of a cyber-attack or a conventional attack) since military necessity allows so. This leads to the essential question as to whether the principle of necessary suffering should be differently envisioned in cyberspace: for instance, by requiring combatants to evaluate if a less than lethal quantumof force can be employed against a cyber-warrior, which might translate in the obligation to capture, rather than kill a cyber-combatant, or to employ non-lethal cybernetic means instead. However, as I have already pointed out in Chapter 1, when I briefly examined the principle of unnecessary suffering and the debate surrounding section IX of the ICRC’s Guidance, this is an extremely contentious issue within IHL, as it basically amounts to a complete reshaping of the principle of distinction and its underlying logic. Addressing all these different legal issues represents, in my opinion, the priority for any endeavour aimed at further humanizing the conduct of hostilities in cyberspace. Having that said, while this thesis has discussed how the humanization process can be perfected through interpretation, I am also aware of the fact that there is only so much that interpretation can do. Despite the fact that States have been, so far, both silent and reluctant in finding a consensus as to how the *jus in bello* should apply to cyberspace, I believe that norm-creation remains most impactful way to pave the road ahead for the protection of human dignity in cyberspace.

# Bibliography.

##

## **Journal Articles.**

Blum G., ‘The Laws of War and the “Lesser Evil”’ 35 *Yale Journal of International Law* (2010) 1.

Boothby W.H., ‘And for Such Time as: The Time Dimension of Direct Participation in Hostilities’ 42 *Ney York Journal of International Law and Policy* (2010) 741.

Bowett D., ‘Reprisals involving recourse to armed force’ (1972) 66 *American Journal of international Law*.

Bring O., ‘International Humanitarian Law after Kosovo: is *Lex Lata* Sufficient?’ 71 *Nordic Journal of International Law* (2002) 39.

Buchan R., ‘Cyberwarfare and the Status of Anonymous under International Humanitarian Law’ (2016) *Chinese Journal of International Law* (15) 741.

Carnahan, B.M., ‘Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity’ 92 (2) *American Journal of International Law* (1998).

Cassese A., ‘The Martens Clause: Half a Loaf or Simply Pie in the Sky?’ 11 (1) *European Journal of International Law* (2000) 187.

Del Mar K., ‘The Requirement of ‘belonging’ under International Humanitarian Law’ 21 (1) *European Journal of International Law* (2010) 105.

Dinniss H. H., ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ 48 (1) Israel Law Review (2015) 39.

Downey W.G., ‘The Laws of War and Military Necessity’ 47 (2) *American Journal of International Law* (1953)252.

Doyle J., ‘Computer Networks, Proportionality, and Military Operations’ 76 *International Law Studies* (2002) 147.

Droege C., ‘Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians’ 94 *International Review of the Red Cross* No. 886 (2012).

Dunbar C., ‘Military Necessity in War Crimes Trials’, 19 *British Yearbook of International Law* (1952) 442.

Fabre C., ‘Guns, Food and Liability to Attack in War’ 120 *Ethics* (2009) 36.

Fenrick W.J., ‘Attacking the Enemy Civilian as a Punishable Offense’ 7 *Duke Journal of Comparative and International Law* (1997)539.

Fleck D., ‘Strategic Bombing and the Definition of Military Objectives’ 27 *Israel Yearbook on Human Rights* (1997) 48.

G.I.A.D. Draper, ‘Military Necessity and Humanitarian Imperatives’ 12 *Military Law and the Law of War Review* (1973) 135.

Geiss R., ‘The Principle of Proportionality: Force Protection as Military Advantage’ 45 (I) *Israel Law Review* (2012) 71.

Geiss R., Lahmann H., ‘Cyber Warfare: applying the principle of distinctions in an interconnected space’ 45 *Israel Law Review* (3) 381.

Goodman R., ‘The Obama Administration and Targeting ‘’War Sustaining’’ Objects in Noninternational Armed Conflict’ 110 (4) *American Journal of International Law* (2016) 663

Goodman R., ‘The Power to Kill or Capture Enemy Combatants’ 24 *European Journal of International Law* (2013) 819.

Green J.A., ‘The *ratione temporis* elements of self-defence’ 2(1) *Journal on the Use of Force and International Law* (2015) 97.

Gross O., Ni Aolain F., ‘Emergency, War and International Law – Another Perspective’ 70 (1) *Nordic Journal of International Law* (2001) 29.

Hayashi N., ‘Contextualizing Military Necessity’, 27 *Emory International Law Review* (2010) 192.

Hayashi N., ‘Requirements of Military Necessity in International Humanitarian Law and in International Criminal Law’ 28 *Boston University International Law Journal* (2013) 39.

Hays Parks W., ‘Part IX of the ICRC ‘Direct Participation in Hostilities’ Study: No Mandate, No Expertise, and Legally Incorrect’ 42 *New York Journal of International Law and Politics* (2010) 770.

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

Huang Z., Mačák K., ‘Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches’ 16 *Chinese Journal of International Law* (2017) 271.

Husack D.N. ‘Justifications and the Criminal Liability of Accessories’ 80 *Journal of Criminal Law and Criminology* (1989-1990) 491.

Jennings R., ‘The Caroline and McLeod cases’ 32 (1) *American Journal of International Law* (1938) 82.

Jensen E.T., ‘Cyber Attacks: Proportionality and Precautions in Attack’ 89 *International Law Studies* (2013) 198.

Kelsey J., ‘Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare’ 106 *Michigan Law Review* (2008) 1427.

Kilovaty I., ‘ICRC, NATO and the U.S. – Direct Participation in *Hacktivities* – Targeting Private Contractors and Civilians in Cyberspace under International Humanitarian Law’ 15 *Duke Law and Technology Review* (2016) 1.

Kleffner J., ‘From ‘Belligerents’ to ‘Fighters’ and Civilians Directly Participating in Hostilities –On the Principle of Distinction in Non-International Armed Conflicts One Hundred Years after the Second Hague Peace Conference’ 14 *Netherlands International Law Review* (2007) 315.

Kleinig J., Evans N., ‘Human Dignity, Human Flourishing and Human Rights’ 35 (5) *Law and Philosophy* (2015) 549.

Laursen A., ’NATO, the War over Kosovo, and the ICTY Investigation’ 17 *American University International Law Review* (2002) 76.

Lazar S., ‘Necessity in Self-Defence and War’40 *Philosophy & Public Affairs* (2012) 3.

Luban D., ‘Military Necessity and the Cultures of Military Law’ 26(2) *Leiden Journal of International Law* (2013) 315.

Lubell N., ‘Lawful Target in Cyber Operations: Does the Principle of Distinction Apply?’ 89 *International Law Studies* 252 (2013).

Mačák K., ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’, 48 (1) *Israel Law Review* (2015) 55.

Margalit, A. and Walzer, M., ‘Israel, Civilian and Combatants’ 56 (8) *New York Review of Books* (2009).

McCrudden C., ‘Human Dignity and Judicial Interpretation of Human Rights’ 19 *European Journal of International Law* (4) (2008) 655.

Melzer N., ‘Keeping the Balance Between Military Necessity and Humanity: A response to Four Critiques of the ICRC’s Interpretive Guidance on the notion of Direct Participation in Hostilities’ 42 *New York Journal of International Law and Policy* (2010) 833.

Meron T., ‘The Humanization of International Humanitarian Law’ 94 (2) *American Journal of International Law* (2000) 239.

Meron T., ‘The Martens Clause, Principles of Humanity, and Dictates of Public Conscience’, 94 (1) *American Journal of International Law* (2000) 78.

Padmanabhan V., ‘Cyber Warriors and the *Jus in Bello*’ 89 *International Law Studies* (2013) 288.

Padmanabhan V., ‘Cyberwarriors and the *Jus in Bello’* 89 *International Law Studies* (2013) 288.

Richmond D., ‘Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications of the Law of Armed Conflict?’ 35 *Fordham International Law Journal* (2012) 842.

Rid, T., Mc Burney, P. ‘Cyber-Weapons’, 157 *RUSI Journal* (1), (February 2012) 6.

Robinson I., Nohle E., ‘Proportionality and precautions in attack: The reverberating effects of using explosive weapons in populated areas’ 98(1) *International Review of the Red Cross* (2016) 107.

Rowe P., ‘Kosovo 1999: The Air Campaign – Have the Provisions of Additional Protocol I Withstood the Test?’ 837 *International Review of the Red Cross* (2000).

Sassoli M., Quintin A., ‘Active and Passive Precautions in Air and Missile Warfare’ 44 *Israel Yearbook of Human Rights* (2014) 69.

Schachter O., ‘Human Dignity as a Normative Concept’ 77 *American Journal of International Law* (1983) 853.

Schmitt M. N., ‘Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance’50 *Virginia Journal of International Law* (2010) 795.

Schmitt M. N., ‘Precision Attack and International Humanitarian Law’ 87 (859) *International Review of the Red Cross* (2005) 445.

Schmitt M., ‘Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees’ 5 *Chicago Journal of International Law* (2004-2005). 521.

Schmitt M.N, ‘The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis’ 1 *Harvard National Security Law Journal* (2010)34.

Schmitt M.N., ‘Deconstructing Direct Participation in Hostilities: The Constitutive Elements’ 42 *New York Journal of International Law and Politics* (2010) 697.

Schmitt M.N., ‘Wired Warfare: Computer Network Attack and *Jus in Bello*’ 84 *International Review of the Red Cross* (2002) 365.

Sensen O., ‘Human dignity in historical perspective: the contemporary and traditional paradigms’ 10 (1) *European Journal of Political Theory* (2011) 71.

Shany Y, Efrony D., ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice’ 112 (4) *American Journal of International Law* (2018) 583.

Sharp T., et al. ‘Exploring the psychological and somatic impact of identity theft’ 49 *Journal of Forensic Sciences* (2004) 131.

Shue H., Whippman D., ’Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions’ 35 *Cornell International Law Journal* (2002) 559.

Sloane R., ‘Puzzles of Proportion and the ‘’Reasonable Military Commander’’: Reflections on the Law, Ethics, and Geopolitics of Proportionality’ 6 *Harvard National Security Journal* (2015) 299.

Solis G., ‘Targeted Killing and the Law of Armed Conflict’ 60 *Naval War College Review* (2007).

T. McCormack, ‘International Humanitarian Law and the Targeting of Data’ 94 *International Law Studies* (2018) 222.

Talbot Jensen E., ‘Cyber-Attacks: Proportionality and Precautions in Attack’ in 89 *International Law Studies* (2013) 198.

Talbot Jensen E., ‘Cyberwarfare and Precautions against the effects of attacks’ 88 *Texas Law Review* (2010)1532.

Talbot Jensen E., ‘Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?’18 (5) *American University International Law Review* (2005)1145.

Tsagourias N., ‘Necessity and the Use of Force: A Special Regime’, Dekker F., Hey E. (eds.), *Netherlands Yearbook of International Law Volume 41* (2010)11.

Turns D., ‘Cyber Warfare and the Notions of Direct Participation in Hostilities’ 17 *Journal of Conflict and Security Law* No. 2 (2012) 279.

Venturini G., ‘Necessity in the Law of Armed Conflict and International Criminal Law’ *41 Netherlands Yearbook of International Law* (2010) 45.

Wallace D., Reeves S.H.,‘The Law of Armed Conflict ‘Wicked’ Problem: *Levee en Masse* in Cyber Warfare’ 89 *International Law Studies* (2013) 646.

Watkin K., ‘Opportunity Lost: Organized Armed Groups and the ICRC ‘Direct Participation in Hostilities’ Interpretive Guidance’ 42 *New York Journal of International Law and Politics* (2009-2010) 641.

Watts S., ‘Combatant Status and Computer Network Attack’ 50 (2) *Virginia Journal of International Law* (2010) 392.

Watts, S., ‘Combatant Status and Computer Network Attack’ 50 *Virginia Journal of International Law* No. 2 (2010) 392.

Yehuda R., ‘Post-Traumatic Stress Disorder’, 346 *New England Journal of Medicine* (2002) 108.

Zhang L., ‘A Chinese perspective on cyber war’ 94 (886) *International Review of the Red Cross* (2012) 802.

Zohar N., ‘Double Effect and Double Intention: A Collectivist Perspective’ 40 *Israel Law Review* (2007) 730.

## **Books.**

A.P.V. Rogers, *Law on the Battlefield* (Manchester University Press 1996).

Boothby W.H., Von Heinegg W.H., *The Law of War: A detailed Assessment of the US Department of Defense Law of War Manual* (Cambridge University Press 2018).

Borghesi F., (ed.), *Pico Della Mirandola: Oration on the Dignity of Man* (Cambridge University Press 2012.

Bothe M., Partsch K.J., Solf W. (eds.), *New Rules for Victims of Armed Conflict* (International Committee of the Red Cross, 1982).

Brierly J.L., *The Law of Nations* (Oxford, Clarendon Press 1963).

Cicero, *De Officis*, tr. W. Miller (Harvard University Press 1913).

Crawford E., [The Treatment of Combatants and Insurgents under the Law of Armed Conflict](http://www.oxfordscholarship.com/view/10.1093/acprof%3Aoso/9780199578962.001.0001/acprof-9780199578962) (Oxford University Press 2010).

Crawford J., *The International Law Commission’ Articles on State Responsibility*: *Introduction, Text and Commentaries* (Cambridge University Press 2002).

Da Costa, K., *The Extraterritorial Application of Selected Human Rights Treaties* (Martinus Nijhoff 2013).

De Preux J., *Geneva Convention Relative to the Treatment of Prisoners of War: Commentary* (ICRC, 1960).

Dinniss H.H., *Cyber Warfare and the Laws of War* (Cambridge University Press 2011).

Dinstein Y., *The Conduct of Hostilities under the Law of International Armed Conflict* (third edition, Cambridge University Press 2016).

Dinstein Y., *War, Aggression and Self-Defence* (Cambridge University Press (sixth edition, Cambridge University Press 2017).

Dunant H., *A Memory of Solferino* (ICRC 1986).

Fuller J.F.C., *The Conduct of War 1789-1961* (Eyre & Spottiswoode 1962).

Gardam J., *Necessity, Proportionality and the Use of Force by States* (Cambridge University Press 2004).

Gilabert P., *Human Dignity and Human Rights* (Oxford University Press 2018).

Greenspan M., *The Modern Law of Land Warfare* (University of California Press 1959).

Griffin J., *On Human Rights* (Oxford University Press 2008).

Grotius H., *De Jure Belli ac Pacis (On the Law of War and Peace) (*1625) (Francis W. Kelsey Transl. 1925).

Harvard University, Program on International Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Harvard 2009).

Henckaerts J.M., Doswald-Beck L., *Customary International Humanitarian Law* (ICRC, Cambridge 2005).

Henckaerts J-M., Doswald-Beck L/, *Customary International Humanitarian Law*, International Committee of the Red Cross (Cambridge University Press 2005).

Henderson I., *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Brill 2009).

Jachec-Neale A.*, The Notion of Military Objective in International Law and Targeting Practice* (Routledge 2014).

Kalshoven F., Zegveld L., *Constraints on the Waging of War: An Introduction to International Humanitarian Law* (Fourth edition, International Committee of the Red Cross2011).

Kant I., Groundwork *of the Metaphysic of Morals*, trans. Mary Gregor (Cambridge University Press, 1998).

McMahan J., *Killing in War* (Oxford University Press 2009).

Melzer N., *Cyberwarfare and International Law*, UNIDIR (2011).

Melzer N., *Targeted Killing in International Law* (Oxford University Press 2008).

Melzer, N., *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009).

Milanovic M., *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press 2011).

Nathanson S., *Terrorism and the Ethics of War* (Cambridge University Press 2010).

Ohlin J.D., *Necessity in International Law (*Oxford University Press 2016).

Paddeu F., *Justification and Excuse in International Law* (Oxford University Press 2017).

Park I., *The Right to Life in Armed Conflict* (Oxford University Press 2018).

Pictet J., *Development and Principles of International Humanitarian Law* (Martinus Nijhoff 1985).

Pilloud *C.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12th August 1949 (*Martinus Nijhoff 1987).

Roberts A., Guelff R. (eds.) *Documents on the Laws of War* (Oxford University Press 1998).

Roscini M., *Cyber Operation and the Use of Force in International Law,* Oxford University Press (2015) p. 181.

Ruys T., *Armed Attack and Article 51 of the UN Charter: Evolution in Customary Law and Practice* (Cambridge University Press 2011).

Schmitt M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

Schmitt, M.N. (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

Walzer M., *Just and Unjust Wars*: *A Moral Argument with Historical Illustrations* (Basic Books 2015).

Witt J.F., Lincoln’s *Code: The Laws of War in American History* (Free Press Editions, 2012).

## **Chapters in Edited Volumes.**

Amer El-Din, ‘The Protection of the Civilian Population’ in Ronzitti N., Venturini G., (eds.), *The Law of Air Warfare: Contemporary Issues* *I* (Eleven International Publishing 2006) 28.

Arai-Takahashi Y., ‘Proportionality’ in Shelton D., (ed.) *The Oxford Handbook of International Human Rights Law* (Oxford University Press 2013).

Bannerlier-Christakis C., ‘Is the principle of distinction still relevant in cyberwarfare? ‘in N. Tsagourias and R.J. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar (2015) 343.

Bussolati N., ‘The Rise of Non-State Actors in Cyberwarfare’ in Ohlin J.D., Govern K., and Finkelstein C. (eds.) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 102.

Cannizzaro E., ‘The Principle of Proportionality’, in Clapham A., Gaeta P. (eds.) *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press 2014) 223.

Coady C.A.J., ‘Collateral Immunity in War and Terrorism’ in Primoraz I., (ed.) *Civilian Immunity in War* (Oxford University Press 2007) 136.

Dederer H. and Singer T., ‘Adverse Cyber Operations: Causality, Attribution, Evidence and Due Diligence’ 95 *International Law Studies* (2019) 430.

Dicke K., ‘The Founding Function of Human Dignity in the Universal Declaration of Human Rights’ in Kreztmer D., Klein E., (eds.) *The Concept of Dignity in Human Rights Discourse* (Kluwer Law International 2002)118.

Dinstein Y. ‘The Principle of Proportionality’ in Mujezinovic-Larssen K., Guldahl-Cooper C., Ntsuyen G. (eds.) *Searching for a Principle of Humanity in International Humanitarian Law* (Cambridge University Press 2012) 72.

Garraway C., ‘The Changing Character of the Participants in War: Civilianization of Warfighting and the concept of ‘Direct Participation in Hostilities’ in 87 *International Law Studies – International Law and the Changing Character of War* (2010) 177.

Greenwood C., ‘Customary International Law and the First Geneva Protocol of 1977 in the Gulf Conflict’ in Rowe P.J. (ed.), *The Gulf War 1990-1991* *in International and English Law* (Routledge, London, 1993) 374.

Greenwood C., ‘Historical Development and Legal Basis’ in Fleck, D. (ed.) *Handbook of International Humanitarian Law* (Oxford University Press 2008)130.

Gross M. et al. ‘Immune from Cyber-fire? The Psychological and Physiological Effects of Cyberwar’ in Allhoff F. et al. (eds.) *Binary Bullets: The Ethics of Cyberwarfare* (Oxford University Press, 2018) p. 8.

Holliss D. B., ‘Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?’ in Ohlin J.D., Govern K., Finkelstein C. (eds.) *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 129.

Kolb R., ‘The Main Epochs of Modern International Humanitarian Law since 1864 and their related dominant legal constructions’ in Mujezinovic-Larssen, K., Guldahl-Cooper C., Ntsuyen, G. (eds.) *Searching for a Principle of Humanity in International Humanitarian Law* (Cambridge University Press 2012) 23.

Lieblich E., ‘Beyond Life and Limb: Exploring Incidental Mental Harm under International Humanitarian Law’ in Jinks D., Maogoto J.N., Solomon S., (eds.), *Applying International Humanitarian Law in Judicial and Quasi-Judicial Bodies: International and Domestic Aspects*, (T.M.C. Asser Press 2014) 185.

Noll G., ‘The Main Epochs of modern International Humanitarian Law since 1864 and their related dominant legal constructions’ in Mujezinovic Larsen K., Guldahl Cooper K., Nystuen G. (eds.) *Searching for a ‘Principle of Humanity in International Humanitarian’ Law* (Cambridge University Press 2012)23.

Oeter S., ‘Collateral Damages – Military Necessity and The Right to Life’ in Tomuschat C., Lagrange S., Oeter S., (eds.), *The Right to Life* (Martinus Nijhoff 2010)167.

Oeter S., ‘Is the Principle of Distinction Outdated?’ in Heintschel von Heinegg W., Epping V. (eds.) *International Humanitarian Law Facing New Challenges* (Springer 2007) 58.

Oeter S., ‘Methods and Means of Combat’ in Fleck D., (ed.), *The Handbook of International Humanitarian Law in Armed Conflicts* (Oxford University Press 2008) 157.

Sassoli M., Cameron L., ‘The Protection of Civilian Objects – Current State of the Law and Issues *De Lege Ferenda*’ in Ronzitti N., Venturini G. (eds.), *The Law of Air Warfare – Contemporary Issues* (Eleven Publishing 2006) 35.

Shue H., ’Proportionality in War’ in Martel G., *The Encyclopaedia of War* (Wiley-Blackwell 2012) 6.

Tsagourias N., ‘The constitutional role of general principles of law in international and European jurisprudence’ in Tsagourias N. (ed.) *Transnational Constitutionalism* (Cambridge University Press 2007) 71.

Waldron J., ‘Is Dignity the Foundation of Human Rights?’ in Cruft R., Liao M., Renzo M. (eds.) *Philosophical Foundations of Human Rights* (Oxford University Press 2015) 118.

## **Blogs, Magazines and Websites.**

Alam N, ‘The Great Bangladesh Cyber Heist Shows Truth is Stranger than Fiction’, *Dhaka Tribune* (March 12, 2016) <<https://www.dhakatribune.com/uncategorized/2016/03/12/the-great-bangladesh-cyber-heist-shows-truth-is-stranger-than-fiction>> accessed 10 October 2019.

Barnes J.E., Gibbons-Neff T., ‘US Carried Out Cyberattacks on Iran’, *The New York Times* (22 June 2019) <https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html> accessed 26 October 2019.

Broad W., Sanger, J., David, E., ‘Israeli Tests on Worm Called Crucial in Iran Nuclear Delay’, *New York Times* (15 January 2011) < <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>> accessed 13 September 2019.

CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations’, *Dragos Inc*. <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf> accessed 12 September 2019.

 F. Anderson, ‘Iran’s Internet blackout: what is happening, and why did the government turn it off?’ The Telegraph (23 November 2019) < <https://www.telegraph.co.uk/news/2019/11/23/irans-internet-blackout-happening-did-government-turn/>> accessed 29 November 2019.

Falliere N., ‘Exploring Stuxnet’s PLC Infection Process’, *Symantec Official Blog* (21 September 2010) <https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process> accessed 12 September 2019.

Falliere N., et al., ‘W.32.Stuxnet Dossier, version 1.4’, *Symantec* (February 2011) <https://www.symantec.com/content/en/us/enterprise/media/security\_response/whitepapers/w32\_stuxnet\_dossier.pdf> accessed 12 September 2019.

Gambrell J., ‘Saudi Arabia Warns Destructive Computer Virus Has Returned’, *AP News* (24 January 2017) <<https://apnews.com/888029171f0e4a67bdbae98cbd5bf814/Saudi-Arabia-warns-destructive-computer-virus-has-returned>> accessed 30 September 2019.

Gilbert D., ‘Anonymous Continues Cyber-Attacks on Israeli Government Websites Knocking Mossad and IDF Offline’, *International Business Times* (4 August 2014) <www.ibtimes.co.uk/anonymous-continues-cyber-attacks-israeli-government-websites-knocking-mossad-idf-offline-1459689> accessed 11 September 2019.

Greenberg A., ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’, *Wired* (1 September 2018) <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 12 September 2019.

Greenberg, A., ‘Crash Override’: The Malware That Took down a Power Grid’, *Wired* (6 December 2017) <www.wired.com/story/crash-override-malware/> accessed 12 September 2019.

Groll E., ‘*NSA* Official Suggests North Korea Was Culprit in Bangladesh Bank Heist’, *Foreign Policy* (21 March 2017) <<https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/>> accessed 10 October 2019.

Internet Blackouts: Reaching for the Kill Switch’, *The Economist* (10 February 2011).

Joby W., ‘Iran’s Nuclear Facilities Recover Quickly from Stuxnet Cyberattack’ *The Washington Post*, (16 February 2011).

Katz Y., ‘Stuxnet might have destroyed 1000 centrifuges at Natanz’, *Jerusalem Post* (24 December 2010) <<https://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz>> accessed 15 October 2019.

Krastouk J., ‘Avast Reports on WannaCrypt0r 2.0 Ransomware that Infested NHS and Telefonica’, *Avast Security News*, (12 May 2017) <blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today> accessed 12 September 2019.

Kumar M., ‘Stuxnet Source Code Released Online’, *The Hacker News* (3 July 2011) <<https://thehackernews.com/2011/07/stuxnet-source-code-released-online.html>> accessed 25 October 2019.

Lee R.M., Assante M. J., Conway T,, ‘German Steel Mill Cyber Attack’, *Sans ICS* (30 December 2014)<<https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>> accessed 12 September 2019.

Leyden M, ’Hack on Saudi Aramco Hit 30,000 Workstations, Oil Firm Admits’, *REGISTER* (29 August 2012) < <https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/>> accessed 1 October 2019.

Nakashima E., ‘Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say’, *Washington Post* (July 9, 2015) <https://www.washingtonpost.com/news /federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-millionpeople-federal-authorities-say/> accessed 20 October 2019.

Noman H., ‘The Emergence of Open and Organized Pro-Government Cyber-Attacks in the Middle East: The Case of Syrian Electronic Army’, *OpenNet Initiative* <<https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-amy>> accessed 7 October 2019.

Polityuk P., ‘Ukraine Investigates Suspected Cyber-attack on Kiev Power Grid’, *Reuters* (20 December 2016).

Roguski P., ‘An Overview of International Humanitarian Law in France’s New Cyber Document’, *Just Security* (27 September 2019) <<https://www.justsecurity.org/66318/an-overview-of-international-humanitarian-law-in-frances-new-cyber-document/>> accessed 1 November 2019.

Schmitt M. N., ‘France Speaks Out on IHL and Cyber Operations: Part II’, *EJIL:Talk!* (1 October 2019) <<https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/>> accessed 1 November 2019.

Serjoie K.A., *Iran Investigates if Series of Oil Industry Accidents Were Caused by Cyber Attack*, TIME (12 August 2016). Available athttps://time.com/4450433/iran-investigates-if-series-of-oil-industry-accidents-were-caused-by-cyber-attack; see also *Iran Oil Industry Fires, Blasts Raise Suspicion of Hacking*, FOX NEWS (22 September 2016) <<https://www.foxnews.com/world/iran-oil-industry-fires-blasts-raise-suspicions-of-hacking>> accessed 10 October 2019.

Shamoon virus targets energy sector infrastructure’, *BBC News* (17 August 2012) <www.bbc.com/news/technology-19293797> accessed 12 September 2019; Symantec Security Response, ‘The Shamoon Attacks’ *Symantec Official Blog*, (16 August 2012) <www.symantec.com/connect/blogs/shamoon-attacks> accessed 12 September 2019.

Stuxnet Worm Hits Iran Nuclear Plant Staff Computers, *BBC NEWS* (26 September 2010). <<https://www.bbc.com/news/world-middle-east-11414483>> accessed 8 October 2019.

Sukumar, A. ‘The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?’ (*Lawfare*, 4 July 2017), <www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well> accessed 26 October 2019.

Syrian Electronic Army: Assad’s Cyber-Warriors’, *The Guardian* (29 April 2013) <<https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background>> accessed 7 October 2019.

Tikk E,.Kaska K., Runnimeri K., Kert M.,Taliharm A.,Vihuul L., *Cyber-attacks against Georgia: Legal Lessons Identified* (CCDCOE, November 2008) < <https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/>> accessed 10 October 2019.

Traynor I. ’Russia Accused of Unleashing cyberwar to disable Estonia’, *The Guardian* (17 May 2007) <www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 10 September 2019.

Unprecedented' cyberattack hits 200,000 in at least 150 countries, and the threat is escalating’, *CNBC* (17 May 2017).

US Department of Homeland Security, CISA Cyber + Infrastructure, *Understanding Denial-of-Service Attacks*, <www.us-cert.gov/ncas/tips/ST04-015> accessed 10 September 2019.

Wang S., Nagaraja S., ‘Pulling the Plug: A Technical Review of the Internet Shutdown in Burma’, *Open Net Initiative* (22 October 2007) < <https://opennet.net/research/bulletins/013>> accessed 25 October 2019.

Weinberger S., ‘How Israel Spoofed Syria’s Air Defense System’, *Wired*, (10 April 2007) <<https://www.wired.com/2007/10/how-israel-spoo/>> accessed 22 October 2019.

 Zetter K., ‘A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever’, *Wired* (8 January 2015) < <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>> accessed 12 September 2019.

Zetter K., ‘Inside the Cunning, Unprecedented Hack on Ukraine’s Power Grid’, *Wired* (3 March 2016) < <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>> accessed 1 October 2019.

## **Reports.**

Ago R., *Addendum – Eight Report on State Responsibility*, A/CN.4/318/Add.5-7 (Yearbook of the International Law Commission 2008)69.

Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia, ICTY.

Human Rights Watch, *Why They Died: Civilian Casualties in Lebanon During the 2006 War*, September 5, 2007. <<https://www.hrw.org/report/2007/09/05/why-they-died/civilian-casualties-lebanon-during-2006-war>> accessed 15 April 2019.

Krug E. G. et al. (eds.), *World Report on Violence and Health*, World Health Organization (2002) 3 <<http://www.who.int/violence_injury_prevention/violence/world_report/en/>> accessed 19 October 2019.

*Off Target: The conduct of the War and Civilian Casualties in Iraq*, Human Rights Watch (December 2003).

Report of the International Law Commission on the Work of Its Thirty-Second Session, UN Doc. A/35/10 (5 May-25 July 1980).

Report on the Work of the Conference; Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Second Session Geneva 3 May-3 June 1972 (ICRC, Geneva, 1972).

State of Israel, *The 2014 Gaza Conflict* (*7 July-26 August 2014): Factual and Legal Aspects* (May 2015).

UN Congress, ‘UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials’; Human Rights Committee, ‘Concluding Observations on Israel’, UN Doc CCPR/CO/78/ISR (2003).

Un Human Rights Council, Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council Resolution S-2/1, A/HRC/3/2 (23 November 2006).

UN Human Rights Council, Report of the United Nations Fact-Finding Mission on the Gaza Conflict, UN Doc.A/HRC/12/48 (25 September 2009).

UNGA ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013) A/68/98\*.

## **Other national and international documents.**

Chairman, Joint Chiefs of Staff, Joint Publication 3-60: Joint Targeting, at II-35 (2007).

Council of the European Union, *Council Directive 2008/114/EC on the identification and designation of European National Infrastructures and the assessment of the need to improve their protection’* (8 December 2008).

Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011).

*The UK National Security Strategy, Protecting and Promoting the UK in a Digital World* (November 2011).

The Vice Chairman of the US, Joint Chiefs of Staff, *Memorandum for Chiefs of the Military Services Commanders, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates* (18 Jan 2012).

UK Ministry of Defence, *The Joint Services Manual of the Law of Armed Conflict* (2004).

US Department of Defense, Office of the General Counsel, *Law of War Manual* (May 2016).

US NAVY, *The Commander’s Handbook on the Law of Naval Operations* (August 2017).

US. Department of Defense, The Vice Chairman of the Joints Chiefs of Staff, *Joint Terminology for Cyberspace Operations* (Nov. 2010).

## **National and International Cases.**

### **European Court of Human Rights.**

*Al Jedda v. The United Kingdom*, App. No 27021/08 (ECtHr, 7 July 2011).

*Al Skeini v. United Kingdom*, App. No 55721/07 (ECtHr, 7 July 2011).

*Handyside v. The United Kingdom* App. No 5493/72 (ECtHr, 7 December 1976).

*Gulec v. Turkey*, App. No. 54/1997/838/1044 (ECtHr, 27 July 1998).

*Lozidou v. Turkey*, App. No 15318/89 (ECtHr,23 March 1995); *Cyprus v. Turkey*, App. No 25781/94 (ECtHr, 10 May 2001).

*Markovic and Others v. Italy*, App. No 1398/03 (ECtHr, 14 December 2006).

*McCann and others V. The United Kingdom* App. No 18984/91 (ECtHr, 27 September 1995).

*Nachova and Others v. Bulgaria*, App, No 43577/98 and 43579/98 (ECThR6 July 2005).

*Öcalan v. Turkey*, App. No 46221/99 (ECtHr, 12 May 2005 *Al Skeini v. United Kingdom*, App. No 55721/07 (ECtHr, 7 July 2011).

### **International Court of Justice.**

*Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43

*Corfu Channel Case*, Judgment on Preliminary Objections, I.C. J. Reports 1948, p. 15.

*Dispute regarding Navigational and Related Rights* (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009, p. 213.

*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, I. C. J. Reports 2004, p. 136.

*Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226.

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

*Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment, I.C.J. Reports, p. 161.

### **International Criminal Court.**

*Prosecutor v Thomas Lubanga Dyilo*, (Judgment) ICC-01/04-01/06-803 (29 February 2007).

### **International Criminal Tribunal for the Former Yugoslavia.**

*Prosecutor v Blaskic* (Judgment) IT-95-14 (3 March 2000).

*Prosecutor v Galic* (Judgment) IT-98-29-T, Judgment (5 December 2003).

*Prosecutor v Jadranko Prlić, Bruno Stojić, Slobodan Praljak, Milivoj Petković, Valentin Ćorić and Berislav Pušić* (Judgment) IT-04-74-A (29 November 2017).

*Prosecutor* *v Kordic and Cerkez* (Judgment) IT-95-14/2-A (7 December 2004).

*Prosecutor v Kupreskic et al*. (Judgment) IT-95-16-T (14 January 2000).

*Prosecutor v Martic* (Review of the Indictment under Rule 61) IT-95-11 (13 September 1996).

*Prosecutor v Strugar* (Decision on Interlocutory Appeal) IT-01-41-AR72 (22 November 2002)

*Prosecutor v Strugar* (Decision on Interlocutory Appeal) IT-01-41-AR72 (22 November 2002).

*Prosecutor v. Blagojevic* (Judgment) IT-02-60-T (17 January 2005).

*Prosecutor v. Delalic et al.*, (Appeals Chamber Judgment) IT-96-21-A (20 February 2001).

*Prosecutor v. Dusko Tadić* (Appeals Chamber Decision) IT-94-1-AR72 (2 October 1995) para. 119.

*Prosecutor* *v. Dusko Tadic (*Decision on the Defence Motion on Interlocutory Appeal on Jurisdiction) IT-94-1 (2 October 1995).

*Prosecutor v. Furundzija*, (Judgment) IT-95-17/1-T, T.Ch. II (10 December 1998) para. 183.

*Prosecutor v. Ljube Boskoski and Johan Tarculovski* (Judgement), IT-04-82-T (10 July 2008)

*Prosecutor v.* *Martic*, (Review of the Indictment Pursuant to Rule 60) IT-95-11-R61 (13 Mar 1995).

*Prosecutor v. Stanislav Galic* (Judgment) IT-98-29 (30 November 2003)

*Prosecutor v. Strugar* (Judgment) IT-01-42-A (17 July 2008).

*Prosecutor v. Tolimir* (Judgment) IT-05-88/2- T (11 December 2012).

*Prosecutor v.* *Zoran Kupreskic et al.* (Trial Chamber Judgement) IT-95-16 (14 January 2000).

### **International Criminal Tribunal for Rwanda.**

*Prosecutor v. Kayishema and Ruzindana* (Judgement) ICTR-95-1-T (21 May 1999).

*Prosecutor v. Seromba* (Appeals Chamber Judgment) Case No. ICTR-2001-6-A (12 March 2008).

*Prosecutor v. Ntawukulilyayo* (Judgment) ICTR-05-82-T (28 April 2009).

 *Prosecutor v. Jean-Paul Akayesu* (Trial Judgement), ICTR-96-4-T (2 September 1998).

**Other National and International Cases.**

*Beit Sourik Village Council v. Government of Israel*, HCJ 2056/04, Supreme Court of Israel (21June 2005).

Eritrea-Ethiopia Claims Commission, ‘Partial Award: Western Front, Aerial Bombardment and Related Claims - Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 & 2’ (19 December 2005).

*Inter-American Commission on Human Rights*, Report No. 55/97, Case No. 11.137: Argentina, OEA/ Ser/L/V/II.98, Doc. 38, (6 December 1997)

*Mara’abe v. Prime Minister of Israel*, HCJ 7957/04, Supreme Court of Israel (15 September 2005).

*Maria Fanny Suarez de Guerrero v Colombia* Communication No. 45/1979: Colombia, UN Human Rights Committee (31 March 1982).

*The Public Committee against Torture in Israel v The Government of Israel*, HCJ 769/02, Supreme Court of Israel (11 December 2005).

*United States V. List (Hostages Trial)*, Case No. 7, United States Military Tribunal at Nuremberg (Feb. 19, 1948).

1. US Department of Defense, The Vice Chairman of the Joints Chiefs of Staff, *Joint Terminology for Cyberspace Operations* (Nov. 2010) 3. [↑](#footnote-ref-1)
2. US Department of Homeland Security, CISA Cyber + Infrastructure, *Understanding Denial-of-Service Attacks*, <www.us-cert.gov/ncas/tips/ST04-015> accessed 10 September 2019. [↑](#footnote-ref-2)
3. I. Traynor, ’Russia Accused of Unleashing cyberwar to disable Estonia’, *The Guardian* (17 May 2007) <www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 10 September 2019. [↑](#footnote-ref-3)
4. E. Tikk, K. Kaska, K. Runnimeri, M. Kert, A. Taliharm, L. Vihuul, *Cyber-attacks against Georgia: Legal Lessons Identified* (CCDCOE, November 2008) 4. [↑](#footnote-ref-4)
5. YouTube video posted by Anonymous entitled “Anonymous: Message to Israel and Palestine”, 19 July 2014 <https://www.youtube.com/watch?list =UUJ 7eFTLJ Arv kg DBae1hbllw&v=iyQA3zMg7ZQ>. [↑](#footnote-ref-5)
6. D. Gilbert, ‘Anonymous Continues Cyber-Attacks on Israeli Government Websites Knocking Mossad and IDF Offline’, *International Business Times* (4 August 2014) <www.ibtimes.co.uk/anonymous-continues-cyber-attacks-israeli-government-websites-knocking-mossad-idf-offline-1459689> accessed 11 September 2019. [↑](#footnote-ref-6)
7. H.H. Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2011) 296. [↑](#footnote-ref-7)
8. N. Falliere, et al., ‘W.32.Stuxnet Dossier, version 1.4’, *Symantec* (February 2011) <https://www.symantec.com/content/en/us/enterprise/media/security\_response/whitepapers/w32\_stuxnet\_dossier.pdf> accessed 12 September 2019. [↑](#footnote-ref-8)
9. N. Falliere, ‘Exploring Stuxnet’s PLC Infection Process’, *Symantec Official Blog* (21 September 2010) <https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process> accessed 12 September 2019. [↑](#footnote-ref-9)
10. Ibid. [↑](#footnote-ref-10)
11. R.M. Lee, M.J. Assante, T. Conway, ‘German Steel Mill Cyber Attack’, *Sans ICS* (30 December 2014) <<https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>> accessed 12 September 2019; K. Zetter, ‘A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever’, *Wired* (8 January 2015)< <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>> accessed 12 September 2019. [↑](#footnote-ref-11)
12. K.A. Serjoie, ‘Iran Investigates if Oil Industry Accidents Were Caused by Cyber-Attacks’, *Time* (August 12, 2016) <<https://time.com/4450433/iran-investigates-if-series-of-oil-industry-accidents-were-caused-by-cyber-attack/>> accessed 12 September 2019. [↑](#footnote-ref-12)
13. ‘Shamoon virus targets energy sector infrastructure’, *BBC News* (17 August 2012) <www.bbc.com/news/technology-19293797> accessed 12 September 2019; Symantec Security Response, ‘The Shamoon Attacks’ *Symantec Official Blog*, (16 August 2012) <www.symantec.com/connect/blogs/shamoon-attacks> accessed 12 September 2019. [↑](#footnote-ref-13)
14. K. Zetter, ‘Inside the Cunning, Unprecedented Attack on Ukraine’s Power Grid’*, Wired* (3 March 2016) <www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid> accessed 12 September 2019. [↑](#footnote-ref-14)
15. A. Greenberg, A., ‘Crash Override’: The Malware That Took Down a Power Grid’, *Wired* (6 December 2017) <www.wired.com/story/crash-override-malware/> accessed 12 September 2019. [↑](#footnote-ref-15)
16. ‘CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations’, *Dragos Inc*. <https://dragos.com/wp-content/uploads/CrashOverride-01.pdf> accessed 12 September 2019. [↑](#footnote-ref-16)
17. ‘Unprecedented' cyberattack hits 200,000 in at least 150 countries, and the threat is escalating’, *CNBC* (17 May 2017) [↑](#footnote-ref-17)
18. J. Krastouk, ‘Avast Reports on WannaCrypt0r 2.0 Ransomware that Infested NHS and Telefonica’, *Avast Security News*, (12 May 2017) <blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today> accessed 12 September 2019. [↑](#footnote-ref-18)
19. A. Greenburg, ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’, *Wired* (1 September 2018) <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 12 September 2019. [↑](#footnote-ref-19)
20. J. Kelsey, ‘Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare’ 106 *Michigan Law Review* (2008) 1434-1435. [↑](#footnote-ref-20)
21. T. Rid, P. McBurney, ‘Cyber-Weapons’, 157 *RUSI Journal* (1), (February 2012) 6. [↑](#footnote-ref-21)
22. H. H. Dinniss, *Cyber Warfare* (n 7) 7. [↑](#footnote-ref-22)
23. J.E. Barnes, T, Gibbons-Neff, ‘US Carried Out Cyberattacks on Iran’, *The New York Times* (22 June 2019) <https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html> accessed 26 October 2019. [↑](#footnote-ref-23)
24. UNGA Res 56/19 (7 February 2002) Un Doc A/RES/56/19. [↑](#footnote-ref-24)
25. See in this regard the third GGE Report. UNGA ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013) A/68/98\*. [↑](#footnote-ref-25)
26. A. Sukumar, ‘The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?’ (*Lawfare*, 4 July 2017), <www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well> accessed 26 October 2019. [↑](#footnote-ref-26)
27. See L. Zhang, ‘A Chinese perspective on cyber war’ 94 (886) *International Review of the Red Cross* (2012) 801 at 805; Z. Huang, K. Mačák, ‘Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches’ 16 *Chinese Journal of International Law* (2017) 271 at 297-303. [↑](#footnote-ref-27)
28. M.N. Schmitt (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013). Hereinafter ‘Tallinn Manual’. [↑](#footnote-ref-28)
29. M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017). Hereinafter ‘Tallinn Manual 2.0’. [↑](#footnote-ref-29)
30. *Prosecutor v. Tadic* (Decision on the Defence Motion on Interlocutory Appeal for Jurisdiction) ICTY 94-1 (2 October 1995) para. 70. [↑](#footnote-ref-30)
31. ibid. [↑](#footnote-ref-31)
32. T. Meron, ‘The Humanization of International Humanitarian Law’ 94 (2) *American Journal of International Law* (2000) pp. 239-278. [↑](#footnote-ref-32)
33. Hague Convention Respecting the Laws and Customs of War on Land (The Hague, 29 July 1899) Preamble. [↑](#footnote-ref-33)
34. See in this regard Y. Dinstein, ‘The Principle of Proportionality’ in K. Mujezinovic-Larssen, C. Guldahl-Cooper, G. Ntsuyen, (eds.) *Searching for a Principle of Humanity in International Humanitarian Law* (Cambridge University Press 2012) 72-85. [↑](#footnote-ref-34)
35. *The Corfu Channel Case* *(Merits)*, Judgment, 9 April 1949, ICJ Reports 1949 (‘Corfu Channel’) 22. [↑](#footnote-ref-35)
36. *Case Concerning Military and Paramilitary Activities in Nicaragua and Against Nicaragua (Merits)*, Judgment (27 June 1986) ICJ Reports 1986 (‘Nicaragua) para. 215. [↑](#footnote-ref-36)
37. *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports 1996 (‘Nuclear Weapons’) para. 79. [↑](#footnote-ref-37)
38. *Prosecutor v.* *Zoran Kupreskic et al.* (Trial Chamber Judgement) IT-95-16 (14 January 2000) paras. 525,535. [↑](#footnote-ref-38)
39. *Prosecutor v. Delalic et al.*, (Appeals Chamber Judgment) IT-96-21-A (20 February 2001) paras. 140-143, 149. [↑](#footnote-ref-39)
40. *Prosecutor v.* *Martic*, (Review of the Indictment Pursuant to Rule 60, IT-95-11-R61 (13 Mar 1995) para. 13. [↑](#footnote-ref-40)
41. See generally A. Cassese, ‘The Martens Clause: Half a Loaf or Simply Pie in the Sky?’ 11 (1) *European Journal of International Law* (2000), pp. 187-216, T. Meron, ‘The Martens Clause, Principles of Humanity, and Dictates of Public Conscience’, 94 (1) *American Journal of International Law* (2000) 78-89. [↑](#footnote-ref-41)
42. Y. Dinstein, ‘The Principle of Proportionality’ (n 31) 73. [↑](#footnote-ref-42)
43. ibid. [↑](#footnote-ref-43)
44. N. Tsagourias, ‘The constitutional role of general principles of law in international and European jurisprudence’ in N. Tsagourias (ed.) *Transnational Constitutionalism* (Cambridge University Press 2007) 71 at 76. [↑](#footnote-ref-44)
45. ibid. [↑](#footnote-ref-45)
46. ibid. [↑](#footnote-ref-46)
47. Namely the principles of distinction, proportionality, precaution and unnecessary suffering. [↑](#footnote-ref-47)
48. R. Kolb, ‘The Main Epochs of Modern International Humanitarian Law since 1864 and their related dominant legal constructions’ in Larssenn et al. (eds.), *Searching for a Principle of Humanity*, (n 31) 23 at 25-41. [↑](#footnote-ref-48)
49. Convention (IV) Respecting the Law and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907 (hereinafter ‘Hague Convention IV’) Art. 22. [↑](#footnote-ref-49)
50. Declaration Renouncing the Use, in Times of War, of Explosive Projectiles under 400 grams Weight, Saint Petersburg, 11 December 1896 (‘St. Petersburg Declaration’) Preamble in A. Roberts, R. Guelff (eds.) *Documents on the Laws of War* (third edition, Oxford University Press 1998) 53-57. [↑](#footnote-ref-50)
51. Ibid. [↑](#footnote-ref-51)
52. Geneva Convention for the Amelioration of the Condition of Wounded and Sick in Armed Forces in the Field (12 August 1949) 75 UNTS 31 (‘Geneva Convention I’). [↑](#footnote-ref-52)
53. Geneva Convention for the Amelioration of the Condition of Wounded. Sick and Shipwrecked Members of the Armed Forces at Sea (12 August 1949) 75 UNTS 85 (‘Geneva Convention II’). [↑](#footnote-ref-53)
54. Geneva Convention Relative to the Treatment of Prisoners of War (12 August 1949) 75 UNTS 135 (‘Geneva Convention III). [↑](#footnote-ref-54)
55. Geneva Convention Relative to the Protection of Civilian Persons in Times of War (12 August 1949) 75 UNTS 287 (‘Geneva Convention IV’). [↑](#footnote-ref-55)
56. This is definition of armed conflict provided by the ICTY in the *Tadic* case. See *Prosecutor v. Dusko Tadic (*Decision on the Defence Motion on Interlocutory Appeal on Jurisdiction) IT-94-1 (2 October 1995) para. 70. [↑](#footnote-ref-56)
57. Geneva Conventions I-IV, Common Article 3. [↑](#footnote-ref-57)
58. Protocol Additions to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977) 1125 UNTS 3 (‘API’) Art. 48, Art.52. [↑](#footnote-ref-58)
59. AP I, Art. 51. [↑](#footnote-ref-59)
60. AP I, Art. 57. [↑](#footnote-ref-60)
61. AP I, Art. 57. [↑](#footnote-ref-61)
62. UNSC Res 827 (25 May 1993)UN Doc S/RES/827 (1993). [↑](#footnote-ref-62)
63. UNSC Res 955 (8 November 1994) UN Doc S/RES/955 (1994). [↑](#footnote-ref-63)
64. *Prosecutor v. Dusko Tadić* (Appeals Chamber Decision) IT-94-1-AR72 (2 October 1995) para. 119. [↑](#footnote-ref-64)
65. N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities* *under International Humanitarian Law* (ICRC, May 2009). Hereinafter ‘DPH Guidance’. [↑](#footnote-ref-65)
66. H.H. Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2011). [↑](#footnote-ref-66)
67. M. Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014). [↑](#footnote-ref-67)
68. C. Droege, ‘Get Off My Cloud: Cyber Warfare, International Humanitarian Law and The Protection of Civilians’ 94 *International Review of the Red Cross* No. 886 (2012) 533; R. Geiss and H. Lahmann, “Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space” 45 *Israel Law Review* No. 3 (2012) 381; N. Lubell, “Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?” 89 *International Law Studies* 89 (2013) 252. [↑](#footnote-ref-68)
69. J. Doyle, “Computer Networks, Proportionality, and Military Operations” 76 *International Law Studies* (2002)147; E.T. Jensen, “Cyber Attacks: Proportionality and Precautions in Attack” 89 *International Law Studies* (2013) 198; [↑](#footnote-ref-69)
70. S. Watts, “Combatant Status and Computer Network Attack” 50 *Virginia Journal of International Law* No. 2 (2010) 291D. Turns, “Cyber Warfare and the Notions of Direct Participation in Hostilities” 17 *Journal of Conflict and Security Law* No. 2 (2012) 279; V. Padmanabhan, “Cyber Warriors and the *Jus in Bello*” 89 *International Law Studies* (2013) 288. [↑](#footnote-ref-70)
71. See, for instance, K. Mačák, “Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law”, 48 *Israel Law Review* No.1 (2015)55; H.H. Dinniss, “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives”, ibid 39; M. N. Schmitt, “The Notion of ‘Objects’ during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision”, ibid. 81. [↑](#footnote-ref-71)
72. For a general overview, see M. Roscini, *Cyber Operations and the Use of Force in International Law* (n 67) pp. 33-40. See also H. Dederer and T. Singer, ‘Adverse Cyber Operations: Causality, Attribution, Evidence and Due Diligence’ 95 *International Law Studies* (2019) 430. [↑](#footnote-ref-72)
73. See *infra*, Chapter 4 pp. 109-117. [↑](#footnote-ref-73)
74. B.M. Carnahan, ‘Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity’ 92 (2) *American Journal of International Law* (1998) 213-231; J.F. Witt, *Lincoln’s Code: The Laws of War in American History* (Free Press Editions, 2012). [↑](#footnote-ref-74)
75. Instructions for the Government of Armies of the United States in the Field (hereinafter ‘Lieber Code’). 24 April 1863. [↑](#footnote-ref-75)
76. F. Paddeu, *Justification and Excuse in International Law* (Oxford University Press 2017). [↑](#footnote-ref-76)
77. N. Tsagourias, ‘Necessity and the Use of Force: A Special Regime’, in F. Dekker and E. Hey (eds.) *Netherlands Yearbook of International Law Volume 41* (2010)11, at 13. [↑](#footnote-ref-77)
78. Report of the International Law Commission on the Work of Its Thirty-Second Session, (5 May-25 July 1980), UN Doc. A/35/10, 71; M. Agius, ‘The invocation of Necessity in International Law’ *Netherlands International Law Review* (2009), 95. [↑](#footnote-ref-78)
79. O. Gross, F. Ni Aolain, ‘Emergency, War and International Law – Another Perspective’ 70 (1) *Nordic Journal of International Law* (2001) 29, at. 34. [↑](#footnote-ref-79)
80. N. Tsagourias, ‘Necessity and the Use of Force’ (n 4) 13. [↑](#footnote-ref-80)
81. See infra, on the application of a right of self-preservation on the conduct of hostilities, giving rise to the *Kriegsrason* doctrine. [↑](#footnote-ref-81)
82. In this regard, Brierly observed that the very existence of the principle of self-preservation ‘would destroy the imperative character of any system of law in which it applied, for it makes all obligation to obey the law merely conditional; and there is hardly any act of international lawlessness which it might not be claimed to excuse.’ See J. L.Brierly, *The Law of Nations* (Oxford, Clarendon Press 1963) 404. [↑](#footnote-ref-82)
83. According to Husack, ‘Justifications are defences that arise from acts or proprieties of acts; […] A defendant is justified when is conduct is not legally wrongful […].’ D. N. Husack, ‘Justifications and the Criminal Liability of Accessories’ 80 *Journal of Criminal Law and Criminology* (1989-1990) 491,496. See also F. Paddeu, *Justification and Excuse in International Law* (Oxford University Press 2017) (n 3) 346-349. [↑](#footnote-ref-83)
84. J. Crawford, *The International Law Commission’ Articles on State Responsibility*: *Introduction, Text and Commentaries* (Cambridge University Press 2002) 178. [↑](#footnote-ref-84)
85. See W. H. Boothby, W.H. Von Heinegg, *The Law of War: A detailed Assessment of the US Department of Defense Law of War Manual* (Cambridge University Press 2018) 31. [↑](#footnote-ref-85)
86. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (‘ICCPR’) Art.1. [↑](#footnote-ref-86)
87. UN Human Rights Committee, *Maria Fanny Suarez de Guerrero v Colombia* Communication No. 45/1979: Colombia (31 March 1982) 137. [↑](#footnote-ref-87)
88. UNHRC, ‘Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston’ A/HRC/14/24/Add.6 (28 May 2010) para. 74; UNGA, ‘Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns’ A/68/382 (13 September 2013) para.33; I. Park, *The Right to Life in Armed Conflict* (Oxford University Press 2018) 25. [↑](#footnote-ref-88)
89. UN Congress, ‘UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials’; Human Rights Committee, ‘Concluding Observations on Israel’, UN Doc CCPR/CO/78/ISR (2003), at.15; UNGA, paras. 2 and 4; I. Park, *The Right to Life in Armed Conflict* (n 15) 27. [↑](#footnote-ref-89)
90. See *Maria Fanny de Guerrero* (n 14) 11.5. [↑](#footnote-ref-90)
91. Ibid. at. 13.2. [↑](#footnote-ref-91)
92. J. D. Ohlin, *Necessity in International Law (*Oxford University Press 2016) 124. [↑](#footnote-ref-92)
93. See Y. Arai-Takahashi, ‘Proportionality’ in D. Shelton, (ed.) *The Oxford Handbook of International Human Rights Law* (Oxford University Press 2013) 446-469. [↑](#footnote-ref-93)
94. That is, when force is used ‘in defence of any person from unlawful violence’, ‘in order to effect a lawful arrest or to prevent the escape of a person lawfully detained’, ‘in action lawfully taken for the purpose of quelling a riot or insurrection.’ See Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) Art. 2(2). [↑](#footnote-ref-94)
95. *Handyside v. The United Kingdom* App. No 5493/72 (ECtHr, 7 December 1976) par. 48. [↑](#footnote-ref-95)
96. N. Melzer, *Targeted Killing in International Law* (Oxford University Press 2008) 116. [↑](#footnote-ref-96)
97. *McCann and others V. The United Kingdom* App. No 18984/91 (ECtHr, 27 September 1995) paras. 212-213. [↑](#footnote-ref-97)
98. N. Melzer, *Targeted Killing in International Law* (n 23) 116. [↑](#footnote-ref-98)
99. *Gulec v. Turkey*, App. No. 54/1997/838/1044 (ECtHr, 27 July 1998) par. 71. [↑](#footnote-ref-99)
100. *Nachova and Others v. Bulgaria*, App, No 43577/98 and 43579/98 (ECThR6 July 2005). [↑](#footnote-ref-100)
101. ibid. para. 198. [↑](#footnote-ref-101)
102. United Nations, *Charter of the United Nations* (24 October 1945) 1 UNTS XVI 9 (‘UN Charter’) Art 2 (4). [↑](#footnote-ref-102)
103. *Case Concerning Military and Paramilitary Activities in Nicaragua and Against Nicaragua (Merits)* (Judgment) ICJ Reports 1986 (hereinafter ‘Nicaragua’) par. 34: ‘There can be no doubt that the issues of the use of force and collective self-defence are issues which are regulated both by customary international law and by treaties, in particular by the United Nations Charter.’. [↑](#footnote-ref-103)
104. ICJ, *Nicaragua* (n 30), pp. 100-101, par. 190; International Law Commission, *Draft Articles of the Vienna Convention of the Law od Treaties with Commentaries* (ILC Yearbook, 1966) 247. [↑](#footnote-ref-104)
105. UN Charter, Art. 51. [↑](#footnote-ref-105)
106. Hugo Grotius, *De Jure Belli ac Pacis (On the Law of War and Peace) (*1625) (Francis W. Kelsey Transl. 1925) 175. [↑](#footnote-ref-106)
107. Hugo Grotius, *De Jure Belli ac Pacis* 398. [↑](#footnote-ref-107)
108. J.D. Ohlin, May, L. (ed.) *Necessity in International Law* (Oxford University Press 2016) 28. [↑](#footnote-ref-108)
109. See R. Jennings, ‘The Caroline and McLeod cases’ 32 (1) *American Journal of International Law* (1938) 82 at 92. [↑](#footnote-ref-109)
110. 29 BFSP 1129, 1138 (Webster to Fox) (1841). Available at <[http://avalon.law.yale.edu/19th\_century/br-1842d.asp> accessed](http://avalon.law.yale.edu/19th_century/br-1842d.asp%3E%20accessed)10 September 2019. [↑](#footnote-ref-110)
111. Ibid. [↑](#footnote-ref-111)
112. ICJ, *Nicaragua* (n 33) par. 191. [↑](#footnote-ref-112)
113. As such, acts like a mere frontier incident, or assistance to rebels in the form of the provision of weapons or logistical or other support constitute do not give rise to the right to self-defence, as opposed to an attack carried out by the armed forces of a State. See ICJ, *Nicaragua* (n 30), par. 195. [↑](#footnote-ref-113)
114. Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America) (Judgment) para. 64 (‘Oil Platforms’). [↑](#footnote-ref-114)
115. Y. Dinstein, *War, Aggression and Self-Defence* (Cambridge University Press (sixth edition, Cambridge University Press 2017) 191. [↑](#footnote-ref-115)
116. ibid. [↑](#footnote-ref-116)
117. ibid. [↑](#footnote-ref-117)
118. J. A. Green, ‘The *ratione temporis* elements of self-defence’ 2(1) *Journal on the Use of Force and International Law* (2015) 97 107. [↑](#footnote-ref-118)
119. R. Ago, *Addendum – Eight Report on State Responsibility*, A/CN.4/318/Add.5-7 (Yearbook of the International Law Commission 2008)69. [↑](#footnote-ref-119)
120. T. Ruys, *Armed Attack and Article 51 of the UN Charter: Evolution in Customary Law and Practice* (Cambridge University Press 2011) 97. Hereinafter ‘Armed Attack.’ [↑](#footnote-ref-120)
121. T. Ruys, *Armed Attack* (n 47) 98; see also D. Bowett, ‘Reprisals involving recourse to armed force’, 66 *American Journal of international Law* (1977) 1 at 7. [↑](#footnote-ref-121)
122. T. Ruys, *Armed Attack* (n 47) pp. 99-108. [↑](#footnote-ref-122)
123. Instructions for the Government of Armies of the United States in the Field (hereinafter ‘Lieber Code’) 24 April 1863. [↑](#footnote-ref-123)
124. *United States V. List (Hostages Trial)*, Case No. 7, United States Military Tribunal at Nuremberg (Feb. 19, 1948).

1253. [↑](#footnote-ref-124)
125. N. Melzer, N., *Targeted Killing in International Law* (n 23) 283-286. [↑](#footnote-ref-125)
126. Lieber Code (n 50) Art. 15. [↑](#footnote-ref-126)
127. Lieber Code (n 50) Art. 16. [↑](#footnote-ref-127)
128. D. Luban, ‘Military Necessity and the Cultures of Military Law’ 26(2) *Leiden Journal of International Law* (2013), 315, at 343. [↑](#footnote-ref-128)
129. G. Venturini, ‘Necessity in the Law of Armed Conflict and International Criminal Law’ *41 Netherlands Yearbook of International Law* (2010) 45 at 51. [↑](#footnote-ref-129)
130. St. Petersburg Declaration (n 47) Preamble. [↑](#footnote-ref-130)
131. *Hostage Case* (n 51) 1230. [↑](#footnote-ref-131)
132. G. Solis, ‘Targeted Killing and the Law of Armed Conflict’ 60 *Naval War College Review* (2007) 127, 130.

Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (third edition, Cambridge University Press 2016) 34. [↑](#footnote-ref-132)
133. J.D. Ohlin, *Necessity in International Law* (Oxford University Press 2016) 112. [↑](#footnote-ref-133)
134. M. Bothe, K.J. Partsch, W. Solf, *New Rules for Victims of Armed Conflict* (International Committee of the Red Cross, 1982). [↑](#footnote-ref-134)
135. N. Melzer, *Targeted Killing* (n 23)286-287. [↑](#footnote-ref-135)
136. ibid. [↑](#footnote-ref-136)
137. See C. Dunbar, ‘Military Necessity in War Crimes Trials’, 19 *British Yearbook of International Law* (1952) 442, 444; W.G. Downey, ‘The Laws of War and Military Necessity’ 47 (2) *American Journal of International Law* (1953)252; G.I.A.D. Draper, ‘Military Necessity and Humanitarian Imperatives’ 12 *Military Law and the Law of War Review* (1973) 135; B. McCarnahan, ‘Lincoln, Lieber, and the Laws of War: The Origins and Limits of the Principle of Military Necessity’ 92 *American Journal of International Law* (1998) 216-217; C. Greenwood, ‘Historical Development and Legal Basis’ in Fleck, D. (ed.) *Handbook of International Humanitarian Law* (Oxford University Press 2008),p. 130;Venturini, *Military Necessity* (56); G. Blum, ‘The Laws of War and the “Lesser Evil”’ 35 *Yale Journal of International Law* (2010). [↑](#footnote-ref-137)
138. J.D. Ohlin,’ *Necessity in International Law* (60)101. [↑](#footnote-ref-138)
139. St. Petersburg Declaration (n 47) Preamble. [↑](#footnote-ref-139)
140. N. Melzer., *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, International Committee of the Red Cross, Geneva (2010) (‘DPH Guidance’) p.82. [↑](#footnote-ref-140)
141. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, ICTY para. 74 [↑](#footnote-ref-141)
142. D. Luban, *Military Necessity and the Cultures of Military Law* (n 55) 342. [↑](#footnote-ref-142)
143. See N. Melzer (n 23) 287. [↑](#footnote-ref-143)
144. N. Hayashi, ‘Requirements of Military Necessity in International Humanitarian Law and in International Criminal Law’ 28 *Boston University International Law Journal* (2013) 61-62. [↑](#footnote-ref-144)
145. Convention IV Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907, Art. 23 (g) ((‘Hague Convention IV’) in A. Roberts, R. Guelff (eds.) *Documents on the Laws of War* (n 57) 67. [↑](#footnote-ref-145)
146. GC III, Art. 126. [↑](#footnote-ref-146)
147. GC IV, Art. 49. [↑](#footnote-ref-147)
148. AP I, Art. 54.1. [↑](#footnote-ref-148)
149. G. Venturini, *Military Necessity* (n 56) 53. [↑](#footnote-ref-149)
150. See generally N. Hayashi, ‘Contextualizing Military Necessity’, 27 *Emory International Law Review* (2010) 192, at 262-278. [↑](#footnote-ref-150)
151. See generally N. Hayashi, *Requirements of Military Necessity* (n 71); for further discussion of this version of necessity, see D. Luban, ‘Military Necessity and the Cultures of Military Law’ 26 (2) *Leiden Journal of International Law* (2013) 315 at 345; S. Lazar, ‘Necessity in Self-Defence and War’ (2012), 40 (1) *Philosophy & Public Affairs* (2012) 3. [↑](#footnote-ref-151)
152. *Beit Sourik Village Council v. Government of Israel*, HCJ 2056/04, Supreme Court of Israel (21 June 2005); *Mara’abe v. Prime Minister of Israel*, HCJ 7957/04, Supreme Court of Israel (15 September 2005). [↑](#footnote-ref-152)
153. See *Beit Sourik* (n 79) par. 32. [↑](#footnote-ref-153)
154. ibid. [↑](#footnote-ref-154)
155. For a similar consideration, see M.N. Schmitt, ‘Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance’50 *Virginia Journal of International Law* (2010) 795, at 798. [↑](#footnote-ref-155)
156. See, for instance, Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A (III) (‘UDHR’) Art. 1. [↑](#footnote-ref-156)
157. *Prosecutor v. Furundzija*, (Judgment) IT-95-17/1-T, T.Ch. II (10 December 1998) para. 183. [↑](#footnote-ref-157)
158. UDHR (n 85), Preamble. [↑](#footnote-ref-158)
159. Such as Israel and Germany. [↑](#footnote-ref-159)
160. See J. Waldron, ‘Is Dignity the Foundation of Human Rights?’ in R. Cruft, M. Liao, M. Renzo (eds.) *Philosophical Foundations of Human Rights* (Oxford University Press 2015) 127. See also O. Schachter, ‘Human Dignity as a Normative Concept’ 77 *American Journal of International Law* (1983) 853. [↑](#footnote-ref-160)
161. K. Dicke, ‘The Founding Function of Human Dignity in the Universal Declaration of Human Rights’ in D. Kreztmer, E. Klein, (eds.) *The Concept of Dignity in Human Rights Discourse* (Kluwer Law International 2002)118. [↑](#footnote-ref-161)
162. J. Waldron, (n 88).127. [↑](#footnote-ref-162)
163. Ibid.128. [↑](#footnote-ref-163)
164. O. Sensen, ‘Human dignity in historical perspective: the contemporary and traditional paradigms’ 10 (1) *European Journal of Political Theory* (2011) 71-91, 75-76. [↑](#footnote-ref-164)
165. J. Kleinig, N. Evans, ‘Human Dignity, Human Flourishing and Human Rights’ 35 (5) *Law and Philosophy* (2015) 549. [↑](#footnote-ref-165)
166. C. McCrudden, ‘Human Dignity and Judicial Interpretation of Human Rights’ 19 *European Journal of International Law* (4) (2008) 657. [↑](#footnote-ref-166)
167. Cicero, *De Officiis*, tr. W. Miller (1913). Cambridge, MA: Harvard University Press. [↑](#footnote-ref-167)
168. F. Borghesi, (ed.), *Pico Della Mirandola: Oration on the Dignity of Man* (Cambridge University Press 2012). [↑](#footnote-ref-168)
169. I. Kant, Groundwork *of the Metaphysic of Morals*, trans. Mary Gregor (Cambridge, UK: Cambridge University Press, 1998) 42. [↑](#footnote-ref-169)
170. ICCPR, Art. 10. [↑](#footnote-ref-170)
171. CG I-IV, Common Article 3. [↑](#footnote-ref-171)
172. See P. Gilabert, *Human Dignity and Human Rights* (Oxford University Press 2018) 122. [↑](#footnote-ref-172)
173. ibid. [↑](#footnote-ref-173)
174. J. Griffin, *On Human Rights* (Oxford University Press 2008). [↑](#footnote-ref-174)
175. UDHR (n 86) Art. 23 (2). [↑](#footnote-ref-175)
176. *Öcalan v. Turkey*, App. No 46221/99 (ECtHr, 12 May 2005); *Markovic and Others v. Italy*, App. No 1398/03 (ECtHr, 14 December 2006); *Al Skeini v. United Kingdom*, App. No 55721/07 (ECtHr, 7 July 2011); *Al Jedda v. The United Kingdom*, App. No 27021/08 (ECtHr, 7 July 2011). [↑](#footnote-ref-176)
177. See *Lozidou v. Turkey*, App. No 15318/89 (ECtHr,23 March 1995); *Cyprus v. Turkey*, App. No 25781/94 (ECtHr, 10 May 2001). [↑](#footnote-ref-177)
178. See generally M. Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press 2011). See also K. Da Costa, *The Extraterritorial Application of Selected Human Rights Treaties* ( Martinus Nijhoff 2013). [↑](#footnote-ref-178)
179. ICCPR (n 13) Art. 6. [↑](#footnote-ref-179)
180. ICJ, *Nuclear Weapons* (n 28) para. 25. [↑](#footnote-ref-180)
181. ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, ICJ Reports (2004) para. 106. [↑](#footnote-ref-181)
182. Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (‘AP I’) Art. 48. [↑](#footnote-ref-182)
183. ICJ, *Nuclear Weapons* (n 28), par. 79. [↑](#footnote-ref-183)
184. ICTY, *Prosecutor v Blaskic*, Case No. IT-95-14, Judgment, 3 March 2000, par. 180.; *Prosecutor v Martic*, Case No. IT-95-11, Review of the Indictment under Rule 61, 8 March 1996, par. 10; *Prosecutor v Kordic and Cerkez*, Case No. IT-95-14/2-A, Appeals Judgment, 7 December 2004, par. 54; *Prosecutor v Kupreskic et al*, Case No. IT-95-16-T, Judgment, 14 January 2000, par. 521; Prosecutor *v Galic*, Case No. IT-98-29-T, Judgment, 5 December 2003, par. 27. [↑](#footnote-ref-184)
185. *Prosecutor v Strugar* (Decision on Interlocutory Appeal) IT-01-41-AR72 (22 November 2002) par. 10. [↑](#footnote-ref-185)
186. Inter-American Commission on Human Rights, Report No. 55/97, Case No. 11.137: Argentina, OEA/ Ser/L/V/II.98, Doc. 38, (6 December 1997) para 177 (‘La Tablada Case’). [↑](#footnote-ref-186)
187. See M. Walzer, *Just and Unjust Wars*: *A Moral Argument with Historical Illustrations* (Basic Books 2015); C. Fabre, ‘Guns, Food and Liability to Attack in War’ 120 *Ethics* (2009) 36. [↑](#footnote-ref-187)
188. AP I, Art. 51. [↑](#footnote-ref-188)
189. Geneva Conventions I-IV, Common Art. 3. [↑](#footnote-ref-189)
190. AP I, Arts. 75 and 85. [↑](#footnote-ref-190)
191. AP I, Art. 41; J-M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law* (ICRC, Cambridge 2005) Rule 41. [↑](#footnote-ref-191)
192. See Melzer, N., *DPH Guidance* (n 62) 21-26 and 30-35. [↑](#footnote-ref-192)
193. N. Melzer, *DPH Guidance* (n 62) 41-69. [↑](#footnote-ref-193)
194. N. Melzer *DPH Guidance* (n 62) 65. [↑](#footnote-ref-194)
195. M.N. Schmitt, ‘Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance’ (n 83) 834. [↑](#footnote-ref-195)
196. ibid. [↑](#footnote-ref-196)
197. W. Boothby, ‘And for Such Time as: The Time Dimension of Direct Participation in Hostilities’ 42 *Ney York Journal of International Law and Policy* (2010) 741 at 746-750. [↑](#footnote-ref-197)
198. For a general defence of the ICRC study, see N. Melzer, ‘Keeping the Balance Between Military Necessity and Humanity: A response to Four Critiques of the ICRC’s Interpretive Guidance on the notion of Direct Participation in Hostilities’ 42 *New York Journal of International Law and Policy* (2010)833. [↑](#footnote-ref-198)
199. AP I, Art. 52. [↑](#footnote-ref-199)
200. ibid. [↑](#footnote-ref-200)
201. AP I, Art. 51 (5) (b). [↑](#footnote-ref-201)
202. M. Walzer, *Just and Unjust Wars* (n 113) C.A.J. Coady, ‘Collateral Immunity in War and Terrorism’ in I. Primoraz, (ed.) *Civilian Immunity in War* (Oxford University Press 2007)157; N. Zohar., ‘Double Effect and Double Intention: A Collectivist Perspective’ 40 *Israel Law Review* (2007)730-742 J. McMahan. *Killing in War* (Oxford University Press 2009); S. Nathanson, *Terrorism and the Ethics of War* (Cambridge University Press 2010). [↑](#footnote-ref-202)
203. AP I, Art. 57 (2) (a) (ii). [↑](#footnote-ref-203)
204. AP I, Art. 57 (2) (a) (iii). [↑](#footnote-ref-204)
205. AP I, Art. 57 (2) (a) (b). [↑](#footnote-ref-205)
206. AP I, Art. 57 (3). [↑](#footnote-ref-206)
207. Lazar, S., ‘Necessity in Self-Defense and War’ 40 *Philosophy and Public Affairs* (2012) 3 at. 23. [↑](#footnote-ref-207)
208. ibid. [↑](#footnote-ref-208)
209. ICJ, *Nuclear Weapons* (n 28), para. 227. [↑](#footnote-ref-209)
210. St. Petersburg Declaration (n 47) Preamble. [↑](#footnote-ref-210)
211. Hague Convention IV, Art. 23 (a). [↑](#footnote-ref-211)
212. Hague Declaration Concerning Asphyxiating Gasses, The Hague (29 July 1899). [↑](#footnote-ref-212)
213. Protocol IV to the Convention concerning Certain Conventional Weapons, Article 1. [↑](#footnote-ref-213)
214. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (18 September 1997). [↑](#footnote-ref-214)
215. AP I, Art 54 (1) [↑](#footnote-ref-215)
216. N. Melzer, *DPH* Guidance (n 23) 77-82. Italics added. [↑](#footnote-ref-216)
217. J. Pictet, *Development and Principles of International Humanitarian Law* (Martinus Nijhoff 1985) 75-76. [↑](#footnote-ref-217)
218. N. Melzer, *DPH Guidance* (n 27) 82; R. Goodman, ‘The Power to Kill or Capture Enemy Combatants’ 24 *European Journal of International Law* (2013) 819. [↑](#footnote-ref-218)
219. M.N. Schmitt, ‘Preserving the Delicate Balance’, p. 836. [↑](#footnote-ref-219)
220. W. Hays Parks, ‘Part IX of the ICRC ‘Direct Participation in Hostilities’ Study: No Mandate, No Expertise, and Legally Incorrect’ 42 *New York Journal of International Law and Politics* (2010) 770, at 799-810. [↑](#footnote-ref-220)
221. See the definition of non-international armed conflict given in *Tadic*; Prosecutor *v. Dusko Tadic aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)*, IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995, Par. 70: ‘[…]an armed conflict exists 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.’ [↑](#footnote-ref-221)
222. AP I, Art. 49. [↑](#footnote-ref-222)
223. Vienna Convention on the Law of Treaties (13 May 1969) 1155 UNTS 331 (‘VCLT’) Art. 31. [↑](#footnote-ref-223)
224. Oxford English Dictionary (2nd edition, Oxford University Press 1989). [↑](#footnote-ref-224)
225. E. G. Krug et al. (eds.), *World Report on Violence and Health*, World Health Organization (2002) 3 <<http://www.who.int/violence_injury_prevention/violence/world_report/en/>> accessed 19 October 2019. [↑](#footnote-ref-225)
226. AP. I, Art. 54. [↑](#footnote-ref-226)
227. AP, I, Art. 55. [↑](#footnote-ref-227)
228. AP, I, Art. 51. [↑](#footnote-ref-228)
229. AP, I, Art. 52. [↑](#footnote-ref-229)
230. AP, I, Art. 57. [↑](#footnote-ref-230)
231. M. N. Schmitt, ‘Computer Network Attack and *Jus in Bello*’, 84 *International Review of the Red Cross* (2002) (‘Computer Network Attack’) 377. [↑](#footnote-ref-231)
232. AP I, Art. 56. [↑](#footnote-ref-232)
233. The Vice Chairman of the US Joint Chiefs of Staff, *Memorandum for Chiefs of the Military Services Commanders, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates* (18 January 2012) 3. [↑](#footnote-ref-233)
234. H.H. Dinniss, ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ 48 (1) Israel Law Review (2015), p. 41 (hereinafter ‘The Nature of Objects’). [↑](#footnote-ref-234)
235. ibid. [↑](#footnote-ref-235)
236. ibid. [↑](#footnote-ref-236)
237. Chairman, Joint Chiefs of Staff, Joint Publication 3-60: Joint Targeting, at II-35 (2007). [↑](#footnote-ref-237)
238. ibid. [↑](#footnote-ref-238)
239. K. A. Serjoie *Iran Investigates if Series of Oil Industry Accidents Were Caused by Cyber Attack*, TIME (12 August 2016). Available athttps://time.com/4450433/iran-investigates-if-series-of-oil-industry-accidents-were-caused-by-cyber-attack; see also *Iran Oil Industry Fires, Blasts Raise Suspicion of Hacking*, FOX NEWS (22 September 2016). Available at https://www.foxnews.com/world/iran-oil-industry-fires-blasts-raise-suspicions-of-hacking. Quoted in Y. Shany, D. Efrony, ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice’ 112 (4) *American Journal of International Law* (2018) 583-657. [↑](#footnote-ref-239)
240. Stuxnet Worm Hits Iran Nuclear Plant Staff Computers, *BBC NEWS* (26 September 2010). Available at <https://www.bbc.com/news/world-middle-east-11414483>. [↑](#footnote-ref-240)
241. I. Traynor, Russia Accused of Unleashing Cyberwar to Disable Estonia, *The Guardian* (17 May 2007). Available at https://www.theguardian.com/world/2007/may/17/topstories3.russia. [↑](#footnote-ref-241)
242. N. Alam, ‘The Great Bangladesh Cyber Heist Shows Truth is Stranger than Fiction’, *Dhaka Tribune* (March 12, 2016) <<https://www.dhakatribune.com/uncategorized/2016/03/12/the-great-bangladesh-cyber-heist-shows-truth-is-stranger-than-fiction>> accessed 11 October 2019; see also E. Groll, ‘*NSA* Official Suggests North Korea Was Culprit in Bangladesh Bank Heist’, *Foreign Policy* (21 March 2017) <https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/> accessed 11 October 2019. [↑](#footnote-ref-242)
243. M. N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)p.106; M. N. Schmitt, *Tallinn Manual* 2.0 *on the International Law Applicable to Cyberspace Operations* (Cambridge University Press 2017) 415. [↑](#footnote-ref-243)
244. M. N. Schmitt (ed.), *Tallinn Manual 1.0* (n 22), 107; see also M.N. Schmitt (ed.) *Tallinn Manual 2.0* (n 22) 416. [↑](#footnote-ref-244)
245. C. Bannerlier-Christakis, ‘Is the principle of distinction still relevant in cyberwarfare? ‘in N. Tsagourias and R.J. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar (2015) 343 at 348. [↑](#footnote-ref-245)
246. M. N. Schmitt (ed.), *Tallinn Manual 2.0* (n 22) 416. [↑](#footnote-ref-246)
247. M. N. Schmitt (ed.), *Tallinn Manual 1.0* (n 22) 106. [↑](#footnote-ref-247)
248. ibid. 126. [↑](#footnote-ref-248)
249. ibid. at 126-127. [↑](#footnote-ref-249)
250. C. Pilloud, C*.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12th August 1949 (*Martinus Nijhoff 1987), paras. 2007-208 (hereinafter ‘Commentary on the Additional Protocols’). [↑](#footnote-ref-250)
251. M. N. Schmitt (ed.) *Tallinn Manual* 2.0 (n 22) 417. [↑](#footnote-ref-251)
252. M. N. Schmitt (ed.), *Tallinn Manual 1.0* (n 22)108-109. [↑](#footnote-ref-252)
253. Consider, however, that the causation of psychological harm could lead to a different conclusion. See *infra*, Section IV. [↑](#footnote-ref-253)
254. M.N. Schmitt (ed.) *Tallinn Manual 1.0* (n 22) 168. [↑](#footnote-ref-254)
255. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Document Prepared by the International Committee of the Red Cross for the 32nd International Conference of the Red Cross and Red Crescent, Geneva, 8-10 December 2015*, 97 *International Review of the Red Cross* (2016) 1427, 1478. [↑](#footnote-ref-255)
256. ibid. [↑](#footnote-ref-256)
257. M.N. Schmitt (ed.), *Tallinn Manual 2.0* (n 22) 437. Italics added. [↑](#footnote-ref-257)
258. C. Droege, ‘Get off my Cloud: cyber warfare, international humanitarian law, and the protection of civilians’ 94 *International Review of the Red Cross* (2012) 533, p. 557; N. Lubell, ‘Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?’ 89 *International Law Studies* (2013) 252 at 264. [↑](#footnote-ref-258)
259. Ibid. [↑](#footnote-ref-259)
260. C. Droege, *Get off my Cloud* (n 37) 558. [↑](#footnote-ref-260)
261. Ministère Des Armées, *Droit Internationale Applique aux Operàtions Dans le Cyberspace* (2019) <<https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf>> accessed 1 November 2019. [↑](#footnote-ref-261)
262. P. Roguski, ‘An Overview of International Humanitarian Law in France’s New Cyber Document’, *Just Security* ( 27 September 2019) <<https://www.justsecurity.org/66318/an-overview-of-international-humanitarian-law-in-frances-new-cyber-document/>> accessed 1 November 2019; M. N. Schmitt, ‘France Speaks Out on IHL and Cyber Operations: Part II’, *EJIL:Talk!* (1 October 2019) <<https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/>> accessed 1 November 2019. [↑](#footnote-ref-262)
263. N. Lubell, ‘Lawful Targets in Cyber Operations’ (n 37) 265. [↑](#footnote-ref-263)
264. M.N. Schmitt (ed.)*, Tallinn Manual 2.0* (n 22) 429. [↑](#footnote-ref-264)
265. N. Melzer, *Cyberwarfare and International Law* (UNIDIR 2011) 27. [↑](#footnote-ref-265)
266. Y, Sandoz, C. Swinarski and B. Zimmerman, *Commentary to Additional Protocol I*, para. 1875. [↑](#footnote-ref-266)
267. M. Roscini, *Cyber Operation and the Use of Force in International Law,* Oxford University Press (2015) 181. [↑](#footnote-ref-267)
268. K. Dormann, *Applicability of the Additional Protocols to Computer Network Attacks*, p. 6. Available at https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf. [↑](#footnote-ref-268)
269. See *infra*, par. III.3.c. [↑](#footnote-ref-269)
270. A. Jachec-Neale*, The Notion of Military Objective in International Law and Targeting Practice* (Routledge 2014) 132. [↑](#footnote-ref-270)
271. ibid. 134. [↑](#footnote-ref-271)
272. K. Mačák, ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ 48 (1) *Israel Law Review* (2015) 55 at 70; N. Lubell, ‘Lawful Targets in Cyber Operations’ (n 37) 267. [↑](#footnote-ref-272)
273. *Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua)*, Judgment, I.C.J. Reports 2009, p. 213 (hereinafter ‘Navigational Rights’). [↑](#footnote-ref-273)
274. *Navigational Rights* para. 43. [↑](#footnote-ref-274)
275. *Navigational Rights* para. 45. [↑](#footnote-ref-275)
276. ibid. [↑](#footnote-ref-276)
277. *Navigational Rights* para. 58. [↑](#footnote-ref-277)
278. *Navigational Rights (Costa Rica v Nicaragua)* para. 66. [↑](#footnote-ref-278)
279. *Gabcikovo-Nagymaros Project (Hungary v Slovakia)*, Judgment (1997) ICJ Rep 1997 para.140. [↑](#footnote-ref-279)
280. K. Mačák, ‘Military Objectives 2.0’ (n 51) 73. [↑](#footnote-ref-280)
281. Nuclear *Weapons* (n 28) para 86. [↑](#footnote-ref-281)
282. G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Jan. 4, 1999). [↑](#footnote-ref-282)
283. Panama’s Response to Developments in the Field of Information and Telecommunications in the Context of International Security, G.A. Res. A/57/166/Add.1, at 5 (Aug. 29, 2002). [↑](#footnote-ref-283)
284. N. Lubell, ‘Lawful Target in Cyber Operations: Does the Principle of Distinction Apply?’ 89 *International Law Studies* 252 (2013) at 267-273; I. Kilovaty, ‘Virtual Violence – Disruptive Cyberspace Operations as “Attacks” Under International Humanitarian Law’ 23 *Michigan Telecommunication and Technology Law Review* 113 (2016) at 126-127. [↑](#footnote-ref-284)
285. K. Mačák, ‘Military Objectives 2.0’ (n 49); H.H. Dinniss ‘The Nature of Objects’: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ 48 (1) *Israel Law Review* (2015) 39. [↑](#footnote-ref-285)
286. Dinniss, H.H, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 184; Lubell, N.; ‘Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?’ (n 37) 267. [↑](#footnote-ref-286)
287. Dinniss, *Cyber Warfare and the Laws of War*, Ibid. [↑](#footnote-ref-287)
288. K. Mačák, ‘Military Objectives 2.0’ (n 51) 76. [↑](#footnote-ref-288)
289. ibid. [↑](#footnote-ref-289)
290. ibid. [↑](#footnote-ref-290)
291. ibid. [↑](#footnote-ref-291)
292. ibid. [↑](#footnote-ref-292)
293. M.N. Schmitt, *Tallinn Manual 1.0* (n 22) 91. [↑](#footnote-ref-293)
294. R. Yehuda, ‘Post-Traumatic Stress Disorder’, 346 *New England Journal of Medicine* (2002) 108. [↑](#footnote-ref-294)
295. AP, I, Art. 51 (2). [↑](#footnote-ref-295)
296. Schmitt, M.N., *Tallinn Manual* (n 22)108. Italics added. [↑](#footnote-ref-296)
297. ibid 123. [↑](#footnote-ref-297)
298. ibid. [↑](#footnote-ref-298)
299. ibid. [↑](#footnote-ref-299)
300. *Prosecutor v. Furundzija* (Trial Judgment) ICTY 95-17-1 (10 December 1998) para.162; *Prosecutor v. Delalic et al.* (Trial Judgment) ICTY 96-21-T (16 November 1998) para. 468. [↑](#footnote-ref-300)
301. *Prosecutor v. Limaj et al.* (Trial Judgment) ICTY 03-66 (30 November 2005) para. 236. [↑](#footnote-ref-301)
302. Statute of the International Criminal Tribunal for Rwanda, Art. 4 (2) (b). [↑](#footnote-ref-302)
303. *Prosecutor v. Kayishema and Ruzindana* (Judgement) ICTR-95-1-T (21 May 1999) paras. 110-111. [↑](#footnote-ref-303)
304. ibid.See also *Prosecutor v. Seromba* (Appeals Chamber Judgment) ICTR-2001-6-A (12 March 2008) paras 45-47 (hereinafter ‘Seromba’); *Prosecutor v. Ntawukulilyayo* (Judgment) ICTR-05-82-T (28 April 2009) par. 452. [↑](#footnote-ref-304)
305. *Seromba* para 47. [↑](#footnote-ref-305)
306. *Prosecutor v. Blagojevic* (Judgment) IT-02-60-T (17 January 2005) par. 645; *Prosecutor v. Tolimir* (Judgment)IT-05-88/2- T (12 December 2012) par. 738. [↑](#footnote-ref-306)
307. T. Sharp, et al.’ Exploring the psychological and somatic impact of identity theft’ 49 *Journal of Forensic Sciences* (2004) 131-136. [↑](#footnote-ref-307)
308. M. Gross, M., et al. ‘Immune from Cyber-fire? The Psychological and Physiological Effects of Cyberwar’ in F. Allhoff et al. (eds.) *Binary Bullets: The Ethics of Cyberwarfare* (Oxford University Press, 2018) 8. [↑](#footnote-ref-308)
309. E. Nakashima, ‘Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say’, *Washington Post* (July 9, 2015) <https://www.washingtonpost.com/news /federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-millionpeople-federal-authorities-say/> accessed 20 October 2019. [↑](#footnote-ref-309)
310. M. N. Schmitt, *Tallinn Manual 2.0* (n 22) 410. [↑](#footnote-ref-310)
311. T. McCormack, ‘International Humanitarian Law and the Targeting of Data’ 94 *International Law Studies* (2018) 222 at 238. [↑](#footnote-ref-311)
312. The Vice Chairman of the US Joint Chiefs of Staff, *Memorandum for Chiefs of the Military Services Commanders, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates* (n 1) 5. [↑](#footnote-ref-312)
313. Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011) 15. <<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>> accessed 10 October 2019. [↑](#footnote-ref-313)
314. Council of the European Union, *Council Directive 2008/114/EC on the identification and designation of European National Infrastructures and the assessment of the need to improve their protection’*, 8 December 2008, Art. 2 (a). [↑](#footnote-ref-314)
315. See, for instance, *The UK National Security Strategy, Protecting and Promoting the UK in a Digital World* (November 2011) 9. <<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>> accessed 10 October 2019. [↑](#footnote-ref-315)
316. AP I, Art. 48. [↑](#footnote-ref-316)
317. See Section I.1 of this Chapter. [↑](#footnote-ref-317)
318. S. Watts, ‘Combatant Status and Computer Network Attack’ (2010) *Virginia Journal of International Law* 50 (2), p.437. [↑](#footnote-ref-318)
319. H.H. Dinniss, *Cyber Warfare and The Laws of War* (Oxford University Press 2011) 145, footnote 27, noting press releases by US officials discouraging pro-US hackers from joining the conflicts against Afghanistan and Iran. [↑](#footnote-ref-319)
320. *Prosecutor v. Jean-Paul Akayesu* (Trial Judgement), ICTR-96-4-T (2 September 1998) para. 626. [↑](#footnote-ref-320)
321. *Prosecutor v. Ljube Boskoski and Johan Tarculovski* (Judgement), IT-04-82-T (10 July 2008) paras. 199-2003. [↑](#footnote-ref-321)
322. M.N. Schmitt (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyberspace Operations* (Cambridge University Press 2017) 89. Hereinafter ‘Tallinn Manual 2.0’. [↑](#footnote-ref-322)
323. R. Buchan, ‘Cyberwarfare and the Status of Anonymous under International Humanitarian Law’ (2016) *Chinese Journal of International Law* (15)748 (‘importantly, these factors are regarded as indicative only; not all need to be present in order to conclude that a group is organized. Generally speaking, though, the more of these indicative features are exhibited by the group, the more the group will be regarded as organized. *The exception is the requirement that the group is subject to responsible command, which Article 4(2) specifically identifies as a legal requirement for members of a group to be regarded as combatants in an international armed conflict*.’ Italics added. [↑](#footnote-ref-323)
324. ‘Hacktivists’ are groups of individuals who convey a social or political message through the use of cyber technologies and cyber-operation techniques, such as website defacements or DDOS attacks. [↑](#footnote-ref-324)
325. See, for a similar argument, M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 79. Hereinafter ‘Tallinn Manual 1.0.’ [↑](#footnote-ref-325)
326. Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press 2016) 53. [↑](#footnote-ref-326)
327. M.N. Schmitt, *Tallinn Manual* (n 10) 99. [↑](#footnote-ref-327)
328. H.H. Dinniss, *Cyberwarfare and the Laws of War* (n 4) 148. [↑](#footnote-ref-328)
329. ibid 146. [↑](#footnote-ref-329)
330. ibid. [↑](#footnote-ref-330)
331. M.N. Schmitt, *Tallinn Manual* (n 10) pp. 141-142. [↑](#footnote-ref-331)
332. M.N. Schmitt, *Tallinn Manual* (n 10)100. See also Watts, S., ‘Combatant Status and Computer Network Attack’ (3) 440. [↑](#footnote-ref-332)
333. R. Buchan, *Cyberwarfare and the Status of Anonymous* (n 3) 752. [↑](#footnote-ref-333)
334. M. Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2015) 196; Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press, 2016), 55. [↑](#footnote-ref-334)
335. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits*, Judgment, I.C.J. Reports 1986 (‘Nicaragua’) paras. 109-110. [↑](#footnote-ref-335)
336. *Nicaragua* (n 19) paras. 115-116. [↑](#footnote-ref-336)
337. *Prosecutor v Dusko* *Tadic* (Judgment) IT-94-1-A (15 July 1999) par. 116 (‘Tadic Appeal Chamber). [↑](#footnote-ref-337)
338. *Tadic Appeal Chamber*, par.131. [↑](#footnote-ref-338)
339. *Tadic Appeal Chamber,* par. 131. [↑](#footnote-ref-339)
340. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43 (‘Genocide Case’) 171. [↑](#footnote-ref-340)
341. M. N. Schmitt, *Tallinn Manual* (n 10), p.85; M.N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyberspace Operations* (Cambridge University Press 2017) 404 (‘Tallinn Manual 2.0’). [↑](#footnote-ref-341)
342. J. De Preux, *Geneva Convention Relative to the Treatment of Prisoners of War: Commentary* (ICRC, 1960) p.57. [↑](#footnote-ref-342)
343. K. Del Mar, ‘The Requirement of ‘belonging’ under International Humanitarian Law’ 21 (1) *European Journal of International Law* (2010)105 at 118. [↑](#footnote-ref-343)
344. *Genocide Case* (n 24) para. 405. [↑](#footnote-ref-344)
345. H. Noman, ‘The Emergence of Open and Organized Pro-Government Cyber-Attacks in the Middle East: The Case of Syrian Electronic Army’*, OpenNet Initiative*. Available at <<https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army>> accessed 15 October 2019; see also’Syrian Electronic Army: Assad’s Cyber-Warriors’, *The Guardian*, Available at <<https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background>> accessed 15 October 2019. [↑](#footnote-ref-345)
346. See *infra*, Chapter 4, for an analysis of what amounts to a military objective in cyberspace. [↑](#footnote-ref-346)
347. M. N Schmitt, *Tallinn Manual 2.0* (n 25) 409. [↑](#footnote-ref-347)
348. M. Greenspan, *The Modern Law of Land Warfare* (University of California Press 1959), arguing that ‘[t]he first duty of a citizen is to defend his country, and provided he does so loyally he should not be treated as a marauder or criminal.’ [↑](#footnote-ref-348)
349. N. Melzer, *Cyberwarfare and International Law* (UNIDIR 2011) 34. [↑](#footnote-ref-349)
350. See D. Wallace, S.H. Reeves,‘The Law of Armed Conflict ‘Wicked’ Problem: *Levee en Masse* in Cyber Warfare’ 89 *International Law Studies* (2013) 646. [↑](#footnote-ref-350)
351. Ibid. pp.649-653, providing different examples of *levee en masse*, from the Prussian *Ehrenburg* of 1813 to the 2008 Russian-Georgian conflict. [↑](#footnote-ref-351)
352. AP I, Art 43. [↑](#footnote-ref-352)
353. Y. Dinstein, *The Conduct of Hostilities* (n 11) 52. [↑](#footnote-ref-353)
354. AP I, Art. 44 (3) [↑](#footnote-ref-354)
355. ibid. [↑](#footnote-ref-355)
356. AP I, Art. 44 (4). [↑](#footnote-ref-356)
357. Y. Dinstein, *The Conduct of Hostilities* (n 11) 52-54. [↑](#footnote-ref-357)
358. S. Watts, ‘The Notion of Combatancy in Cyber Warfare’ 2012 *4th International Conference on Cyber Conflict* (2012 NATO CCDCOE Publications, Tallinn) 235 at 240. [↑](#footnote-ref-358)
359. Sandoz, Y., Swinarski, C., Zimmerman, B. (eds.) *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross (1987) para. 1698. [↑](#footnote-ref-359)
360. J. Kleffner, ‘From ‘Belligerents’ to ‘Fighters’ and Civilians Directly Participating in Hostilities –On the Principle of Distinction in Non-International Armed Conflicts One Hundred Years after the Second Hague Peace Conference’ 14 *Netherlands International Law Review* (2007) 315 at. 317. Hereinafter ‘From ‘Belligerents’ to ‘Fighters’. [↑](#footnote-ref-360)
361. J. Kleffner, ‘From ‘Belligerents’ to ‘Fighters’ (n 35) 317. [↑](#footnote-ref-361)
362. G. Noll, ‘The Main Epochs of modern International Humanitarian Law since 1864 and their related dominant legal constructions’ in K. Mujezionovic-Larsen, C. Guldahl Cooper, G. Nystuen. (eds.) *Searching for a ‘Principle of Humanity in International Humanitarian’ Law* (Cambridge University Press 2012) 23 at 38. [↑](#footnote-ref-362)
363. Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (The Hague, 29 July 1899) Art. 1. Hereinafter Hague Convention 1899. [↑](#footnote-ref-363)
364. Hague Convention 1899 (n 48) Art. 2. [↑](#footnote-ref-364)
365. See generally T. Meron, ‘The Martens Clause, Principles of Humanity, and Dictates of Public Conscience’ 94 (1) *American Journal of International Law* (2000) 78; A. Cassese, ‘The Martens Clause: Half a Loaf or Simply Pie in the Sky?’ 11(1) European Journal of International Law (2000),187. [↑](#footnote-ref-365)
366. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (The Hague, 18 October 1907) Art. 2. [↑](#footnote-ref-366)
367. See Common Article 3 to the 1949 Geneva Conventions. [↑](#footnote-ref-367)
368. F. Kalshoven, L. Zegveld, *Constraints on the Waging of War: An Introduction to International Humanitarian Law* (Fourth Edition, International Committee of the Red Cross, 2011) 69. [↑](#footnote-ref-368)
369. J. Kleffner, ‘From ‘Belligerents’ to ‘Fighters’’ (n 35) 322. [↑](#footnote-ref-369)
370. H. Dunant, *A Memory of Solferino* (ICRC 1986) <[http://www.icrc.org/Web/Eng/siteeng0.nsf/htmlall/p0361](http://www.icrc.org/Web/Eng/siteeng0.nsf/htmlall/p0361%29)> accessed 10 November 2019; E. Crawford, [*The Treatment of Combatants and Insurgents under the Law of Armed Conflict*](http://www.oxfordscholarship.com/view/10.1093/acprof%3Aoso/9780199578962.001.0001/acprof-9780199578962) (Oxford University Press 2010) 7. [↑](#footnote-ref-370)
371. J.F.C. Fuller, *The Conduct of War 1789-1961* (Eyre & Spottiswoode 1962) 77. [↑](#footnote-ref-371)
372. C. Garraway, ‘The Changing Character of the Participants in War: Civilianization of Warfighting and the concept of ‘Direct Participation in Hostilities’ in 87 *International Law Studies – International Law and the Changing Character of War* (2010) 177 at 178. [↑](#footnote-ref-372)
373. Sandoz, Y., Swinarski, C., Zimmerman, B. (eds.) *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross (1987) par. 1942. Hereinafter ‘AP I Commentary’. [↑](#footnote-ref-373)
374. U.S. NAVY, THE COMMANDER’S HANBOOK ON THE LAW OF NAVAL OPERATIONS, Ch. 8.2.2. [↑](#footnote-ref-374)
375. U.S. Department of Defense, *Law of War Manual* (2016) Ch. 5.9.3. [↑](#footnote-ref-375)
376. U.K. Ministry of Defence, *The Joint Services Manual of the Law of Armed Conflict* (2004, p.54 at 5.5.3. [↑](#footnote-ref-376)
377. *The Public Committee against Torture in Israel v The Government of Israel*, HCJ 769/02, Supreme Court of Israel (11 December 2005). Hereinafter ‘Targeted Killings Case’ [↑](#footnote-ref-377)
378. ibid*.* par. 1. [↑](#footnote-ref-378)
379. *Targeted Killings Case* (n 51) Reply Brief on Behalf of the Appellants (8 July 2003), at. 206. [↑](#footnote-ref-379)
380. *Targeted Killings Case* (n 51) Supplementary Response on Behalf of the States Attorney’s Office. [↑](#footnote-ref-380)
381. Commentary to Additional Protocol I para. 1679. [↑](#footnote-ref-381)
382. *Targeted Killings* *Case* (n 51) par. 37. [↑](#footnote-ref-382)
383. *Targeted Killings Case* (n 51) paras. 39-40. [↑](#footnote-ref-383)
384. *Prosecutor v. Strugar* (Judgment) IT-01-42-A (17 July 2008) para. 178. [↑](#footnote-ref-384)
385. *Prosecutor v Strugar* (Judgment) IT-01-42-A (17 July 2008) par. 178. [↑](#footnote-ref-385)
386. *Prosecutor v Thomas Lubanga Dyilo*, (Judgment) ICC-01/04-01/06-803 (29 February 2007). [↑](#footnote-ref-386)
387. N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009), 46 (‘DPH Guidance’). [↑](#footnote-ref-387)
388. Ibid. 47. [↑](#footnote-ref-388)
389. N. Melzer, *DPH Guidance* (n 72) 49. [↑](#footnote-ref-389)
390. N. Melzer, *DPH Guidance* (n 72)47 [↑](#footnote-ref-390)
391. Jachec-Neale, A., *The Concept of Military Objective in International Humanitarian Law* *and targeting Practice* (Routledge 2014) 86. [↑](#footnote-ref-391)
392. N. Melzer, *DPH Guidance* (n 72) 48*.* [↑](#footnote-ref-392)
393. ibid. [↑](#footnote-ref-393)
394. ibid*.*: ‘In addition, interference with computer networks through computer network attacks (ACN) or exploitation (CNE) would also met the threshold of harm requirement, as well as wiretapping the adversary’s high command or transmitting tactical targeting information for an attack.’; Schmitt, M. (ed.) *Tallinn Manual* (n 23) 119. [↑](#footnote-ref-394)
395. M.N. Schmitt, ‘Deconstructing Direct Participation in Hostilities: The Constitutive Elements’ 42 *New York Journal of International Law and Politics* (2010) 697 at 718. [↑](#footnote-ref-395)
396. M. N. Schmitt, M.N., *Tallinn Manual* (n 10) 119. [↑](#footnote-ref-396)
397. AP I, Art. 49. [↑](#footnote-ref-397)
398. N. Melzer, *DPH Guidance* (n 72) 50. [↑](#footnote-ref-398)
399. The New York Times, *Cyberattack Hits Ukraine Then Spreads Internationally*, 27 June 2017. [↑](#footnote-ref-399)
400. #  BBC News, NotPetya cyber-attack cost TNT at least $300m, 20 September 2017.

 [↑](#footnote-ref-400)
401. M. Roscini, *Cyber Operations and the Use of Force in International* Law (Oxford University press 2015) 205; Buchan, R., ‘Cyberwarfare and the Status of Anonymous’ (n 8)746: ‘The ICRC’s approach seems anachronistic in the cyber era where cyberspace is now an independent feature of everyday life […] a significant cyber-attack against important civilian cyber infrastructure can cause significant damage as opposed to mere disruption […]’;V. Padmanabhan., ‘Cyberwarriors and the *Jus in Bello’* 89 *International Law Studies* (2013) 288 at 299. [↑](#footnote-ref-401)
402. See Chapter 2 para. 3. [↑](#footnote-ref-402)
403. N. Melzer, *DPH Guidance* (n 72) 51. [↑](#footnote-ref-403)
404. ibid. 52. [↑](#footnote-ref-404)
405. ibid.54. [↑](#footnote-ref-405)
406. ibid. 55. [↑](#footnote-ref-406)
407. M.N. Schmitt, *‘*Deconstructing Direct Participation in Hostilities’ (n 80) 726. [↑](#footnote-ref-407)
408. D. Turns, ‘Cyberwarfare and the Notion of Direct Participation in Hostilities’ 17 (2) *Journal of Conflict and Security Law* (2012)279 at 288. [↑](#footnote-ref-408)
409. H.H. Dinniss, *Cyberwarfare and the Laws of War*  (n 4) 166, where the author notes that ‘While the requirement that there be a direct causal link is uncontroversial, in attempting to delimit a boundary between direct and indirect participation the guidance specifies that the harm must be brought about in ‘one causal step’. This strict standard appears to be an innovation on the part of the ICRC authors of the study, *as neither prior law nor the expert process contains any reference to a one step test*.’ Italics added. [↑](#footnote-ref-409)
410. M.N. Schmitt, ‘Deconstructing Direct Participation in Hostilities’ (n 80) 731; Watkin, K., ‘Opportunity Lost: Organized Armed Groups and the ICRC ‘Direct Participation in Hostilities’ Interpretive Guidance’ 42 *New York Journal of International Law and Politics* (2009-2010)641a t 658, 680. [↑](#footnote-ref-410)
411. N. Melzer, *DPH Guidance* (n 72) 54. [↑](#footnote-ref-411)
412. ibid. [↑](#footnote-ref-412)
413. M.N. Schmitt, *Tallinn Manual* (n 10)121. [↑](#footnote-ref-413)
414. H.H. Dinniss, *Cyberwarfare and the Laws of War* (n 4) 170, adapting by an analogy an argument made by M. Schmitt, ‘Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees’ 5 *Chicago Journal of International Law* (2004-2005) 521. [↑](#footnote-ref-414)
415. W. Broad, J. Sanger, E. David, ‘Israeli Tests on Worm Called Crucial in Iran Nuclear Delay’, *New York Times*, 15 January 2011 < <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>> accessed 13 September 2019. [↑](#footnote-ref-415)
416. Y. Katz, ‘Stuxnet might have destroyed 1000 centrifuges at Natanz’, *Jerusalem Post*, 24 December 2010 <<https://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz>> accessed 15 October 2019. [↑](#footnote-ref-416)
417. V. Padmanabhan, ‘Cyberwarriors and the *Jus in Bello*’ (n 95) 298; Kilovaty, I., ‘ICRC, NATO and the U.S. – Direct Participation in *Hacktivities* – Targeting Private Contractors and Civilians in Cyberspace under International Humanitarian Law’ 15 *Duke Law and Technology Review* (2016) 1 at 14. [↑](#footnote-ref-417)
418. D. Turns, ’Cyberwarfare and the Notion of Direct Participation in Hostilities’ (n 82) 288, noting that ‘it appears doubtful that CW could ever meet the requirement of direct causation for DPH, which suggests that civilians could engage in CW with impunity.’ [↑](#footnote-ref-418)
419. N. Melzer, *DPH Guidance* (n 72) p.58. [↑](#footnote-ref-419)
420. ibid 63. [↑](#footnote-ref-420)
421. ibid pp. 59-60. [↑](#footnote-ref-421)
422. M. Roscini, M., *Cyber Operations and the Use of Force* (n 86) pp. 210-211. [↑](#footnote-ref-422)
423. N. Melzer, *DPH Guidance* (n 72) 60. [↑](#footnote-ref-423)
424. ibid. 66. [↑](#footnote-ref-424)
425. ibid. [↑](#footnote-ref-425)
426. ibid. 67. [↑](#footnote-ref-426)
427. R.J. Buchan, “Cyberwarfare and the status of Anonymous’ (n 8) 767. For a critique of the ‘for such time as’ requirement, see W. Boothby, ‘“And for Such Time as”: The Time Dimension to Direct Participation in Hostilities’ 42 *New York Journal of International Law and Politics* (2009-2010) 741-768. [↑](#footnote-ref-427)
428. R.J. Buchan‚ ’Cyberwarfare and the status of Anonymous ‘(n 8) ibid. [↑](#footnote-ref-428)
429. ibid. [↑](#footnote-ref-429)
430. M.N. Schmitt, *Tallinn Manual 2.0* (n 7) 431. [↑](#footnote-ref-430)
431. N. Melzer, *DPH Guidance* (n 72) 69. [↑](#footnote-ref-431)
432. ibid. In this regard, the notion of ‘continuous combat function’ is what separates a civilian who is directly participating in hostilities from a member of an organized armed group of a non-State party to the conflict. Thus, individuals whose continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities are exercising a continuous combat function. [↑](#footnote-ref-432)
433. N. Melzer, *DPH Guidance* (n 72) 69. [↑](#footnote-ref-433)
434. W. Boothby, ‘“And for Such Time as”: The Time Dimension to Direct Participation in Hostilities’ (n 101); M.N. Schmitt, ‘Deconstructing Direct Participation in Hostilities’ (n 69); K. Watkin, ‘Opportunity Lost: Organized Armed Groups and the ICRC ‘Direct Participation in Hostilities’ Interpretive Guidance’ (n 80). [↑](#footnote-ref-434)
435. N. Melzer, *DPH Guidance* (n 61) 70. [↑](#footnote-ref-435)
436. R.J. Buchan, ‘Cyberwarfare and the Status of Anonymous’ (n 4)768. [↑](#footnote-ref-436)
437. M.N. Schmitt, ‘The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis’ 1 *Harvard National Security Law Journal* (2010), 34. [↑](#footnote-ref-437)
438. M.N. Schmitt, ‘Cyber Operations and the *Jus in Bello*: Key Issues’ in Pedrozo, R.P., Wollschlaeger, D. (eds.) 87 *International Law Studies* (2010) 312. [↑](#footnote-ref-438)
439. AP I, Art. 52 (2). [↑](#footnote-ref-439)
440. AP I, Art. 54. [↑](#footnote-ref-440)
441. AP I, Art. 55. [↑](#footnote-ref-441)
442. AP I, Art. 56. [↑](#footnote-ref-442)
443. United Nations Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (September 1976) 1108 UNTS 151. [↑](#footnote-ref-443)
444. Hague Convention for the Protection of Cultural Property (14 May 1954). [↑](#footnote-ref-444)
445. AP I, Art. 52 (2). [↑](#footnote-ref-445)
446. M.N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyberspace Operations* (Cambridge University Press 2017) 437 (‘Tallinn Manual 2.0’). [↑](#footnote-ref-446)
447. H.H. Dinniss, ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ 48 (1) *Israel Law Review* (2015) 39 (‘The Nature of Objects’); K. Mačák, ‘Military Objectives 2.0; The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ 48 (1) *Israel Law Review* (2015) 55 (‘Military Objectives 2.0’); T. McCormack, ‘International Humanitarian Law and the Targeting of Data’ 94 *International Law Studies* (2018) 222. [↑](#footnote-ref-447)
448. H.H. Dinnis, ‘The Nature of Objects’ (n 9) pp.44-45. [↑](#footnote-ref-448)
449. M.N. Schmitt, ‘The Notion of ‘Objects’ During Cyber Operations: a Riposte in Defence of Interpretive and Applicative Precision’ 48 (1) *Israel Law Review* (2015) 81 at 103 (‘The Notion of ‘Objects’’). [↑](#footnote-ref-449)
450. ibid 104. [↑](#footnote-ref-450)
451. AP I, Art. 51(5) (b). [↑](#footnote-ref-451)
452. For a similar argument, see M. Roscini, *Cyber Operations and the Use of Force in International Law* (Cambridge University Press (Cambridge University Press 2014) 182; M. N. Schmitt, ‘The Notion of ‘Objects’’ (n 11) 104. [↑](#footnote-ref-452)
453. H.H. Dinniss, ‘The Nature of Objects’ (n 9) 50. [↑](#footnote-ref-453)
454. Assuming, of course, that the hardware does not qualify as a military objective in itself (for instance, that would be the case if Stuxnet’s source code is stored in a computer specifically used by the military). [↑](#footnote-ref-454)
455. AP I, Art. 57 (2) (a) (ii). [↑](#footnote-ref-455)
456. AP I, Art. 57 (3). [↑](#footnote-ref-456)
457. See H. H. Dinniss, ‘The Nature of Objects’ (n 8) 52-53. [↑](#footnote-ref-457)
458. S. Oeter, ‘Methods and Means of Combat’ in D. Fleck, (ed.), *The Handbook of International Humanitarian Law in Armed Conflicts* (Oxford University Press 2008) 157. [↑](#footnote-ref-458)
459. See *infra* Section III. [↑](#footnote-ref-459)
460. A. Jachec-Neale, *The Concept of Military Objective in International Humanitarian Law and Targeting Practice* (Routledge 2014) 84 (hereinafter ‘The Concept of Military Objective’). [↑](#footnote-ref-460)
461. Report on the Work of the Conference; Conference of Government Experts on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts (Second Session Geneva 3 May-3 June 1972) ICRC, Geneva, 1972, pp. 145-146. [↑](#footnote-ref-461)
462. A. Jachec-Neale, *The Concept of Military Objective* (n 21)86. [↑](#footnote-ref-462)
463. ibid. [↑](#footnote-ref-463)
464. ibid. [↑](#footnote-ref-464)
465. ibid. [↑](#footnote-ref-465)
466. ibid. [↑](#footnote-ref-466)
467. ibid. [↑](#footnote-ref-467)
468. See generally *Off Target: The conduct of the War and Civilian Casualties in Iraq*, Human Rights Watch, December 2003. [↑](#footnote-ref-468)
469. R. Goodman, ‘The Obama Administration and Targeting ‘’War Sustaining’’ Objects in Noninternational Armed Conflict’ 110 (4) *American Journal of International Law* (2016) 663 at 671 and accompanying footnotes 42-44. [↑](#footnote-ref-469)
470. UN Human Rights Council, Report of the United Nations Fact-Finding Mission on the Gaza Conflict, UN Doc.A/HRC/12/48, 25 September 2009, paras. 961,1018-1021. [↑](#footnote-ref-470)
471. Un Human Rights Council, Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council Resolution S-2/1, 23 November 2006, A/HRC/3/2, par. 144. [↑](#footnote-ref-471)
472. Department of the Navy, Office to the Chief of Naval Operations and Headquarters, U.S. Marine Corps, Department of Homeland Security and U.S. Coast Guard, *The Commander’s Handbook on The Law of Naval Operations* (July 2007) 87. [↑](#footnote-ref-472)
473. U.S. Department of Defense, Office of the General Counsel, *Law of War Manual* (2016), p.206. [↑](#footnote-ref-473)
474. *Annotated Supplement to the Commander’s Handbook on the Law of Naval Operations*, 73 ILS (U.S. Naval War College 1999) p. 403. [↑](#footnote-ref-474)
475. Eritrea-Ethiopia Claims Commission, ‘Partial Award: Western Front, Aerial Bombardment and Related Claims - Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 & 2’ (19 December 2005) XXV *United Nations Reports of International Arbitral Awards* (‘EEC Partial Award’) 291 at 334, para. 119. [↑](#footnote-ref-475)
476. A. Jachec-Neale, *The Concept of Military Objective* (n 21)95. [↑](#footnote-ref-476)
477. Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (third edition, Cambridge University Press 2011) pp. 95-96 (hereinafter ‘The Conduct of Hostilities’). [↑](#footnote-ref-477)
478. A. Jachec-Neale, *The Notion of Military Objective* (n 21)46. [↑](#footnote-ref-478)
479. M.N. Schmitt, M.N., *Tallinn Manua*l 2.0 (n 8) 437. [↑](#footnote-ref-479)
480. Y Dinstein, *The Conduct of Hostilities* (n 38)*,* pp.97. [↑](#footnote-ref-480)
481. A. Jachec-Neale, *The Notion of Military Objective* (n 21) p.62. [↑](#footnote-ref-481)
482. M.N. Schmitt, *Tallinn Manual 2.0* (n 8) 438. [↑](#footnote-ref-482)
483. Dinniss, *The Notion of Objects* (n 9) 48. [↑](#footnote-ref-483)
484. S. Wang, S. Nagaraja, *Pulling the Plug: A Technical Review of the Internet Shutdown in Burma*, Open Net Initiative, 22 October 2007. [↑](#footnote-ref-484)
485. ‘Internet Blackouts: Reaching for the Kill Switch’, *The Economist* (10 February 2011). [↑](#footnote-ref-485)
486. F. Anderson, ‘Iran’s Internet blackout: what is happening, and why did the government turn it off?’ The Telegraph (23 November 2019) < <https://www.telegraph.co.uk/news/2019/11/23/irans-internet-blackout-happening-did-government-turn/>> accessed 29 November 2019. [↑](#footnote-ref-486)
487. AP I, Art 52 (2). [↑](#footnote-ref-487)
488. S. Oeter, ‘Methods and Means of Combat’ in Fleck, D.(ed.), *The Handbook of International Humanitarian Law in Armed Conflicts* (Oxford University Press 2008) 157; I. Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Brill 2009) 52. [↑](#footnote-ref-488)
489. I. Henderson, *The Contemporary Law of Targeting* (n 49) 53. [↑](#footnote-ref-489)
490. EECC Partial Award (36) para. 121. [↑](#footnote-ref-490)
491. Y. Dinstein, *The Conduct of Hostilities* (n 38), p. 93. [↑](#footnote-ref-491)
492. Pilloud et *al.* (eds.), *Commentary to the Additional Protocols* (n 29) para. 2218. [↑](#footnote-ref-492)
493. A. Jachec-Neale, *The Notion of Military Objective* (n 21)117. [↑](#footnote-ref-493)
494. ibid. [↑](#footnote-ref-494)
495. Y. Dinstein, *The Conduct of Hostilities* (n 36). 93. [↑](#footnote-ref-495)
496. ibid. [↑](#footnote-ref-496)
497. A. Jachec-Neale*, A., The Notion of Military Objective* (n 21)132. [↑](#footnote-ref-497)
498. ibid.134. [↑](#footnote-ref-498)
499. AP I Art 57 (2) (iii). [↑](#footnote-ref-499)
500. On the concept of ‘duty to hack’, see D.B. Hollis, ‘Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?’ in Ohlin, J.D., Govern, K., Finkelstein, C. (eds.) *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 129-174. [↑](#footnote-ref-500)
501. AP I, Art. 51 (5) (b). [↑](#footnote-ref-501)
502. AP I, Art. 57. 2 (a) (iii) and (b). [↑](#footnote-ref-502)
503. Statute of the International Criminal Court, Art. 8. [↑](#footnote-ref-503)
504. J-M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, International Committee of the Red Cross (Cambridge University Press 2005), p. 46 (hereinafter ‘Customary International Humanitarian Law’). [↑](#footnote-ref-504)
505. ibid. [↑](#footnote-ref-505)
506. E. Cannizzaro, ‘The Principle of Proportionality’, in A. Clapham, P. Gaeta (eds.) *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press 2014) 223 at 225. [↑](#footnote-ref-506)
507. ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* (hereinafter ‘Report to the Prosecutor’) para. 48. [↑](#footnote-ref-507)
508. Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press 2016) 150 (‘The Conduct of Hostilities’) [↑](#footnote-ref-508)
509. ibid. 154: ‘[In the same vein] the LOIAC principle of proportionality has everything to do with injury/damage to civilians/civilian objects and nothing to do with combatant losses or damage to military objectives. LOIAC does not require any proportionality between combatants’ losses on the two warrying sides.’ [↑](#footnote-ref-509)
510. Additional Protocol I, Art. 35 (2); Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907 (‘Hague Convention IV’), art. 23 (e); J-M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press 2012) 237. [↑](#footnote-ref-510)
511. AP I, Art. 52(2). [↑](#footnote-ref-511)
512. Lt.Col. K.R. Rizer, *Bombing Dual-Use Targets: Legal, Ethical and Doctrinal Perspectives* (2001) 8. [↑](#footnote-ref-512)
513. H. Shue, D. Whippman, ’Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions’ 35 *Cornell International Law Journal* (2002), 559 at. 569. Hereinafter ‘Attacks on Dual-Use Facilities’. [↑](#footnote-ref-513)
514. H. Shue, D. Whippman, ‘Attacks on Dual-Use Facilities’(n 14). 570-572. [↑](#footnote-ref-514)
515. Dinstein, *The Conduct of Hostilities* (n 8) 120; A.P.V. Rogers, *Law on the Battlefield (*Manchester University Press 1996) 111-112; I. Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff 2009) 207. [↑](#footnote-ref-515)
516. United States Department of Defence, *Law of War Manual*, June 2015 (Updated December 2016), p.251, stating that in relation to dual-use objects ‘[..] it will be appropriate to consider in applying the principle of proportionality the harm to the civilian population that is expected from the attack on such a military objective.’ [↑](#footnote-ref-516)
517. A. Jachec-Neale, *The Concept of Military Objective in International Law and Targeting Practice* (Routledge 2014). [↑](#footnote-ref-517)
518. Chairman, Joint Chiefs of Staff, Joint Publication 3-60: Joint Targeting, at II-35 (2007). [↑](#footnote-ref-518)
519. Ibid. [↑](#footnote-ref-519)
520. See Chapter 3. See K. Mačák, ‘Military Objectives 2.0; The Case for Interpreting Computer Data as Objects under International Humanitarian Law 48 (1) *Israel Law Review* (2015) 55. [↑](#footnote-ref-520)
521. Vienna Conventions on the Law of Treaties (23 May 1969) 1155 UNTS 331 (‘VCLT’) Art. 33 (1). [↑](#footnote-ref-521)
522. M. Bothe, K.J. Partsch, W.A., Solf, New *Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff 2013) para. 2.6.2. [↑](#footnote-ref-522)
523. I. Robinson, E. Nohle, ‘Proportionality and precautions in attack: The reverberating effects of using explosive weapons in populated areas’ 98(1) *International Review of the Red Cross* (2016) pp. 107-145, at.113 (hereinafter ‘Reverberating Effects’). [↑](#footnote-ref-523)
524. AP I, Art.55. [↑](#footnote-ref-524)
525. AP I, Art. 54. [↑](#footnote-ref-525)
526. AP I, Art.56. [↑](#footnote-ref-526)
527. Third Review Conference of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Final Declaration, CCW/CONF.III/11, part II (17 November 2006) p.4. [↑](#footnote-ref-527)
528. US Department of the Army (Training and Doctrine Command) Counterinsurgency (COIN) Field Manual (FM), 7-36. [↑](#footnote-ref-528)
529. E. Talbot Jensen, ‘Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?’18 (5) *American University International Law Review* (2005)1145-1188, at 1176-1177; E. Talbot Jensen, ‘Cyber-Attacks: Proportionality and Precautions in Attack’ in 89 *International Law Studies* (2013). 198-217 at 207; C. Droege, ‘Get off My Cloud: Cyber Warfare, International Humanitarian law, and the Protection of Civilians’ 94 (886) *International Review of the Red Cross* (2012) 533-578 at. 572-573; H.H. Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 207-208; M. Roscini, *Cyber Operations and the Use of Force in International Law* (Cambridge University Press 2014) 220-223. [↑](#footnote-ref-529)
530. M.N. Schmitt, M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)472. [↑](#footnote-ref-530)
531. Us Department of Defense, *Law of War Manual*, 5.12.4. [↑](#footnote-ref-531)
532. Eritrea Ethiopia Claims Commission, Partial Award, Central Front, Ethiopia’s Claim 2, para. 101 (hereinafter ‘Ethiopia’s Claim 2). [↑](#footnote-ref-532)
533. Eritrea Ethiopia Claims Commission, Ethiopia’s Claim 2, para. 102. [↑](#footnote-ref-533)
534. Eritrea Ethiopia Claims Commission, Ethiopia’s Claim 2, para. 110. See also E. Cannizzaro (n 5) ‘The Principle of Proportionality’ pp.223-224. [↑](#footnote-ref-534)
535. V. Manzo, ‘Stuxnet and the Dangers of Cyberwar’, *The National Interest* (29 January 2013) [↑](#footnote-ref-535)
536. *Prosecutor v. Stanislav Galic* (Judgment) IT-98-29 (30 November 2003) para. 58. [↑](#footnote-ref-536)
537. State of Israel, *The 2014 Gaza Conflict* (*7 July-26 August 2014): Factual and Legal Aspects* (May 2015) 49 at 317. [↑](#footnote-ref-537)
538. I. Henderson, K. Reece, ‘Proportionality under International Humanitarian Law: The ‘’Reasonable Military Commander’’ Standard and Reverberating Effects’ 51 *Vanderbilt Journal of Transnational Law* (2018) 835 at 845-846. [↑](#footnote-ref-538)
539. M.N. Schmitt, H.H., Dinniss, A. Wingfield, *Computers and War: The Legal Battlefield* (2004) p.9. [↑](#footnote-ref-539)
540. M. Roscini, *Cyber Operations and the use of Force in International Law* (n 29) p.221; Robinson and Nohle, ’Reverberating Effects’ (n 23( 116. [↑](#footnote-ref-540)
541. C. Greenwood, Observations dated 13 November 2003 circulated by the United Kingdom Delegation to CCW Group of Governmental Experts, 17-24 November 2003, cited in Boothby, W., *Cluster Bombs: is there a Case for New Law?* Occasional Paper Series, Program on Humanitarian Policy and Conflict Research, Harvard University, 2005, p.8. [↑](#footnote-ref-541)
542. For a counter argument on this point, see Robinson and Nohle, *Reverberating Effects*, pp. 117-118. [↑](#footnote-ref-542)
543. Dinnis, H.H., *Cyber Warfare and the Laws of War* (Cambridge University Press 2011)206-207; Roscini, *Cyber Operations and the Use of Force in International Law* (n 29).228. [↑](#footnote-ref-543)
544. ICTY, *NATO Committee Report*, para. 18. [↑](#footnote-ref-544)
545. D. Richmond, ‘Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications of the Law of Armed Conflict?’ 35 *Fordham International Law Journal* (2012) 842, at 893. [↑](#footnote-ref-545)
546. M. Kumar, ‘Stuxnet Source Code Released Online’, *The Hacker News* (3 July 2011) <<https://thehackernews.com/2011/07/stuxnet-source-code-released-online.html>> accessed 25 October 2019. [↑](#footnote-ref-546)
547. For a similar argument, see M. Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 221. [↑](#footnote-ref-547)
548. W. Joby, ‘Iran’s Nuclear Facilities Recover Quickly from Stuxnet Cyberattack’ *The Washington Post*, 16 February 2011 [↑](#footnote-ref-548)
549. M. N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)133. [↑](#footnote-ref-549)
550. One example can be a cyber-attack that causes the destruction of a dam or a power plant, whereby terror may result as a reverberating effect of the cyber-attack itself. [↑](#footnote-ref-550)
551. AP I, Art. 55. [↑](#footnote-ref-551)
552. E. Lieblich, ‘Beyond Life and Limb: Exploring Incidental Mental Harm under International Humanitarian Law’ in D. Jinks, J.N. Maogoto, S. Solomon, (eds.), *Applying International Humanitarian Law in Judicial and Quasi-Judicial Bodies: International and Domestic Aspects*, (T.M.C. Asser Press 2014) 185 at 197-200 (hereinafter’ Beyond Life and Limb). [↑](#footnote-ref-552)
553. See references in E, Lieblich, *Beyond Life and Limb* (n 52). 202-203. [↑](#footnote-ref-553)
554. *Prosecutor v Jadranko Prlić, Bruno Stojić, Slobodan Praljak, Milivoj Petković, Valentin Ćorić and Berislav Pušić* (Judgment) IT-04-74-A (29 November 2017) para. 1582 (hereinafter ‘Prosecutor v. Prlić). [↑](#footnote-ref-554)
555. *Prosecutor v. Prlic*, para. 1584. [↑](#footnote-ref-555)
556. *Prosecutor* *v. Prlic*, para. 1583. [↑](#footnote-ref-556)
557. US DoD *Law of War Manual*, at 5.12.2.1: ‘Remote harms resulting from the attack do no need to be considered in a proportionality analysis. For example, the death of an enemy combatant might cause economic harm to his or her family, or the destruction of a tank factory might cause economic harm in the form of lost jobs […].’ [↑](#footnote-ref-557)
558. M. N. Schmitt, *Tallinn Manual* (n 23), p. 133. [↑](#footnote-ref-558)
559. J. Leyden, ’Hack on Saudi Aramco Hit 30,000 Workstations, Oil Firm Admits’, *REGISTER* (29 August 2012). [↑](#footnote-ref-559)
560. Gambrell, J., ‘Saudi Arabia Warns Destructive Computer Virus Has Returned’, *US News* (24 January 2017). [↑](#footnote-ref-560)
561. K. Zetter, ‘Inside the Cunning, Unprecedented Hack on Ukraine’s Power Grid’, *Wired* (3 March 2016). [↑](#footnote-ref-561)
562. P. Polityuk, ‘Ukraine Investigates Suspected Cyber-attack on Kiev Power Grid’, *Reuters* (20 December 2016). [↑](#footnote-ref-562)
563. 2 Response from Norway, “Responses to Document CCW/GGE/X/WG.1/WP.2, Entitled IHL and ERW, Dated 8 March 2005”, CCW/GGE/XI/WG.1/WP.5, 29 July 2005, § 18–19. [↑](#footnote-ref-563)
564. Report of the Iraq Inquiry (2016) 277-278. [↑](#footnote-ref-564)
565. AP I, Art. 52 (2). [↑](#footnote-ref-565)
566. I. Henderson, *The Contemporary Law of Targeting* (n 15) 201-203; M. Roscini, *Cyber Operations and the Use of Force in International Law* (n 43) 224. [↑](#footnote-ref-566)
567. A.P.V. Rogers, *Law on the Battlefield* (Manchester University Press 1996)99. [↑](#footnote-ref-567)
568. A. Laursen, ’NATO, the War over Kosovo, and the ICTY Investigation’ 17 *American University International Law Review* (2002) 76, at 795; J. Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge University Press 2004) 102; I. Henderson, *The Contemporary Law of Targeting* (n 15) 200; Roscini, *Cyber Operations and the Use of Force in International Law* (n 47)226; Y. Dinstein, *The Conduct of Hostilities* (n 8) 134. [↑](#footnote-ref-568)
569. S. Weinberger, ‘*How Israel Spoofed Syria’s Air Defense System’*, *Wired* (10 April 2007) <<https://www.wired.com/2007/10/how-israel-spoo/>> accessed 22 October 2019. [↑](#footnote-ref-569)
570. Sandoz, Y., Zwinarski, C., Zimmerman, B., *Commentary*, para. 2209; see also UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (Oxford University Press 2004) at 5.33.3; Schmitt, *Tallinn Manual* (n 8) 442. [↑](#footnote-ref-570)
571. *Commentary* para.2218. [↑](#footnote-ref-571)
572. U.S. Department of Defense, Office of the General Counsel, *Law of War Manual* (May 2016) 215. [↑](#footnote-ref-572)
573. Office of the Judge Advocate General, Law of Armed Conflict Manual: At the Operational and Tactical Levels, Joint Doctrine Manual, B-GJ-005-104/FP-02 (2001) para.415. [↑](#footnote-ref-573)
574. See A. Roberts, R. Guelff, *Documents on the Laws of War* (Oxford University Press 2000) pp. 500,508. [↑](#footnote-ref-574)
575. Y. Dinstein, *The Conduct of Hostilities* (n 8) 168. [↑](#footnote-ref-575)
576. M.N. Schmitt, ‘Precision Attack and International Humanitarian Law’ 87(859) *International Review of the Red Cross* (2005) 445 at 462. [↑](#footnote-ref-576)
577. S. Oeter, ‘Collateral Damages – Military Necessity and The Right to Life’ in C. Tomuschat, E. Lagrange, S. Oeter, (eds.), *The Right to Life* (Martinus Nijhoff 2010)167. [↑](#footnote-ref-577)
578. S. Oeter, ‘Is the Principle of Distinction Outdated?’ in W. Heintschel von Heinegg, V. Epping (eds.) *International Humanitarian Law Facing New Challenges* (Springer 2007) 58. [↑](#footnote-ref-578)
579. W.J. Fenrick, Attacking the Enemy Civilian as a Punishable Offense’ 7 *Duke Journal of Comparative and International Law* (1997)539, 548–49. [↑](#footnote-ref-579)
580. R. Geiss, ‘The Principle of Proportionality: Force Protection as Military Advantage’ 45 (I) *Israel Law Review* (2012) 71-89, p. 85 (hereinafter ‘Force Protection’). [↑](#footnote-ref-580)
581. ibid. pp.85-86. [↑](#footnote-ref-581)
582. For a critique of this approach see also M. Roscini, *Cyber Warfare and The Use of Force in International Law* (n 47) 225. [↑](#footnote-ref-582)
583. For a similar argument, see R. Geiss, *Force Protection* (n 80)87. [↑](#footnote-ref-583)
584. M. Roscini, *Cyber Warfare and the Use of Force in International Law* (n 47) p.226. [↑](#footnote-ref-584)
585. US Department of the Army, *Counterinsurgency*, FM No 3-24 (December 2006) para. 7-30. [↑](#footnote-ref-585)
586. See generally R. Sloane, ‘Puzzles of Proportion and the ‘’Reasonable Military Commander’’: Reflections on the Law, Ethics, and Geopolitics of Proportionality’ 6 *Harvard National Security Journal* (2015) 299; Y. Dinstein, *The Conduct of Hostilities* (n 8)158; I. Henderson, *The Contemporary Law of Targeting* at 221; Fenrick. W.J., ‘The Rule of Proportionality and Protocol I in Conventional Warfare’ 98 *Military Law Review* (1982) 91 at 102:’The second question posed is what is the meaning of ‘excessive’ as used in Articles 51(5)(b) and 57(2). Since the quantities being measured, civilian losses and military advantage, are dissimilar, it is not possible to establish any reasonably exact proportionality equation between them.’; M. Sassoli, L. Cameron, ‘The Protection of Civilian Objects – Current State of the Law and Issues *De Lege Ferenda*’ in Ronzitti, N., Venturini, G. (eds.), *The Law of Air Warfare – Contemporary Issues* (Eleven Publishing 2006) p. 35-74, pp.64-64; Roscini, *Cyber Operations and The Use of Force in International Law* (n 43) 418. [↑](#footnote-ref-586)
587. H. Shue, ’Proportionality in War’ in G. Martel, *The Encyclopaedia of War* (Wiley-Blackwell 2012) 6, where the author suggests to sort military advantage into the categories of ‘important’, ‘compelling’ and ‘decisive’, and to sort civilian losses as ‘moderate’, ‘severe’ and ‘catastrophic’, arguing that ‘it is excessive to inflict civilian losses of a category higher than the category of military advantage anticipated.’; Margalit, A. and Walzer, M., ‘Israel, Civilian and Combatants’ 56 (8) *New York Review of Books* (2009) , where the authors argue the following: ‘This is the guideline we advocate: conduct your war in the presence of noncombatants on the other side as if your citizens were the noncombatants.’ [↑](#footnote-ref-587)
588. D. Sloane, *Puzzle of Proportion* (n 86) 330-331. [↑](#footnote-ref-588)
589. M. Bothe, K. J. Partsch, W.A. Solf, New *Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (n 22) 352 (‘New Rules for Victims of Armed Conflict’). [↑](#footnote-ref-589)
590. Y. Dinstein, *The Conduct of Hostilities* (n 8) 158. [↑](#footnote-ref-590)
591. D. Fleck, ‘Strategic Bombing and the Definition of Military Objectives’ 27 *Israel Yearbook on Human Rights* (1997) 48. [↑](#footnote-ref-591)
592. See Chapter 6. [↑](#footnote-ref-592)
593. AP I, Art. 57 (2)(a)(ii). [↑](#footnote-ref-593)
594. Compare Y. Dinstein, *The Conduct of Hostilities* (n 8) pp. 159-160,215, I. Henderson, I. *The Contemporary Law of Targeting*, pp. 192-193. [↑](#footnote-ref-594)
595. AP I Art. 57 (1). [↑](#footnote-ref-595)
596. See Boivin, A., *The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare*, University Centre for International Humanitarian Law, 2 (2006), p. 36. [↑](#footnote-ref-596)
597. AP I, Art. 57 (2) (a) (i). [↑](#footnote-ref-597)
598. AP I, Art. 57 (2) (a) (ii) [↑](#footnote-ref-598)
599. AP I, Art. 57 (2) (a)(iii) [↑](#footnote-ref-599)
600. AP I, Art. 57 (2) (b). [↑](#footnote-ref-600)
601. AP I. Art. 57 (2) (c). [↑](#footnote-ref-601)
602. AP I, Art. 57 (3). [↑](#footnote-ref-602)
603. See *Challenges of 21st Century* *Warfare,* p. 93. [↑](#footnote-ref-603)
604. Schmitt, M.N. (ed.) *The Tallinn Manual* (n 23), Commentary to Rule 52, p. 138. [↑](#footnote-ref-604)
605. International Committee of the Red Cross, *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts* (1974–1977) Vol. XV, 277 (‘CDDH/XV’) 285; W. Fenrick, ‘The Rule of Proportionality in and Protocol I in Conventional Warfare’ 98 *Military Law Review* (1982) 91. [↑](#footnote-ref-605)
606. US Department of Defense, *Law of War Manual* (2016), par. 5.2.3.2. [↑](#footnote-ref-606)
607. Protocol III annexed to the Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to have Indiscriminate Effects (hereinafter ‘CCW Convention’), Art. 1 (5). [↑](#footnote-ref-607)
608. M.N. Schmitt, ‘Precision Attack and International Humanitarian Law’ 87 (859) *International Review of the Red Cross* (2005) 445 at 462. [↑](#footnote-ref-608)
609. See I. Henderson, *The Contemporary Law of Targeting* (Martinus Nijhoff 2009)162. [↑](#footnote-ref-609)
610. R. Guelff, A. Roberts, *Documents on the Laws of War* (Oxford University Press 1998), Spanish Declaration E, 509. [↑](#footnote-ref-610)
611. In the cyber domain, ‘exploits’ are ‘subsidiary software programs that take advantage of vulnerabilities in computer systems or surrounding networks’. See T. Herr, 13 (1) *The Journal of Information Warfare* (2014) 1 at 6. [↑](#footnote-ref-611)
612. ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* (‘NATO Final Report’) par 29*.* [↑](#footnote-ref-612)
613. See Canada *LOAC Manual* (1999), quoted in J-M. Henckaerts, L. Doswald-Beck, (eds.) *Customary International Humanitarian La*w*,* vol. II (2005) 364. [↑](#footnote-ref-613)
614. I. Henderson, *The Contemporary Law of Targeting* (n 15) p. 163 provides this example. [↑](#footnote-ref-614)
615. ICTY, *Prosecutor v Galic* (Trial Chamber), Case No IT-98-29-T (5 December 2003) par. 51. [↑](#footnote-ref-615)
616. See *The Public Committee against Torture in Israel v The Government of Israel*, HCJ 769/02 (13 December 2006) [5] (Rivlin V-P). [↑](#footnote-ref-616)
617. I. Henderson, *The Contemporary Law of Targeting* (n 15) 165. [↑](#footnote-ref-617)
618. See H.H. Dinniss, *Cyberwarfare and the Laws of War* (Oxford University Press 2011) 212. [↑](#footnote-ref-618)
619. Network mapping is a technique used to ‘discover and visualize physical and virtual network connectivity via a group of interrelated tasks that facilitate the creation of a network map, including flowcharts, network diagrams, topology (i.e., IP detection) and device inventory.’ See Techopedia, Network Mapping, available at <https://www.techopedia.com/definition/29783/network-mapping> (retrieved 28 March 2019). [↑](#footnote-ref-619)
620. Footprinting is a technique used for gathering information about computer systems and the entities they belong to. See SearchSecurity, Footprinting, available at <https://searchsecurity.techtarget.com/definition/footprinting> (retrieved 28 March 2019). [↑](#footnote-ref-620)
621. US Presidential Policy Directive/PPD-20, 20 October 2012, p.7. See Roscini, M. Cyber Operations and the Use of Force in International Law (Oxford University Press 2015) 235. [↑](#footnote-ref-621)
622. H.H Dinniss, *Cyber Warfare and the Laws of War* (n 24) 210. [↑](#footnote-ref-622)
623. AP I, Art. 52 (3). [↑](#footnote-ref-623)
624. E. Talbot Jensen, ‘Proportionality and Precautions in Attack’ 89 *International Law Studies* (2013) 198 at 210. [↑](#footnote-ref-624)
625. F. Kalshoven, L-, Zegveld, *Constraints on the Waging of War* (ICRC 2001) 108. [↑](#footnote-ref-625)
626. I. Henderson, *The Contemporary Law of Targeting* (n 15) 168. [↑](#footnote-ref-626)
627. ibid. [↑](#footnote-ref-627)
628. See *Needless Deaths in the Gulf War: Civilian Casualties During the Air Campaign and Violations of the Laws of War* (1991) Human Rights Watch (2 March 2005). [↑](#footnote-ref-628)
629. See International Law Association Study Group on the Conduct of Hostilities in the 21st Century, *The Conduct of Hostilities Under International Humanitarian Law: Challenges of 21st Century Warfare*, 93 *International Law Studies* (2017) 322 at 383-384. [↑](#footnote-ref-629)
630. Harvard University, Program on International Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Harvard 2009), Rule 8. [↑](#footnote-ref-630)
631. H.H. Dinniss, *Cyber Warfare and the Laws of War* (n 24) 213; see also M. Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 235. [↑](#footnote-ref-631)
632. M.N. Schmitt, ‘Wired Warfare: Computer Network Attack and *Jus in Bello*’ 84 (846) *International Review of the Red Cross* (2002) 365 at 384. [↑](#footnote-ref-632)
633. It must be pointed out that with cyber-attacks there is the risk that, once employed, the defending party may adopt cyber-defence to prevent cyber-attacks of the same time from happening. This is an important factor that needs to be taken into account in determining the military advantage gained from launching a cyber-attackinstead of a kinetic attack. For a similar argument, see H.H. Dinniss, *Cyberwarfare and the Laws of War* (n 24). 213. [↑](#footnote-ref-633)
634. M. Roscini, *Cyber Operations and the Use of Force in International Law* (n 37) 235. [↑](#footnote-ref-634)
635. Fenrick, D., ‘The Rule of Proportionality and Protocol I in Conventional Warfare’ (n 11) 109. [↑](#footnote-ref-635)
636. A logic bomb is ‘malicious programming code which is inserted into application software or an operating system. The code lies dormant until a predetermined period of time has elapsed, or a triggering event (or a series of events) occurs, at which time the code activates.’ [↑](#footnote-ref-636)
637. AP I, Art. 57 (2) (c). [↑](#footnote-ref-637)
638. Human Rights Watch, *Why They Died: Civilian Casualties in Lebanon During the 2006 War*, September 5, 2007. <<https://www.hrw.org/report/2007/09/05/why-they-died/civilian-casualties-lebanon-during-2006-war>> accessed 15 April 2019. [↑](#footnote-ref-638)
639. UK Ministry of Defense, *Manual of the Law of Armed Conflict* (2004) Art. 5.32.8. [↑](#footnote-ref-639)
640. M. Sassoli, A. Quintin, ‘Active and Passive Precautions in Air and Missile Warfare’ 44 *Israel Yearbook of Human Rights* (2014) pp. 69-132, p. 109. [↑](#footnote-ref-640)
641. O. Bring, ‘International Humanitarian Law After Kosovo: is *Lex Lata* Sufficient?’ 71 *Nordic Journal of International Law* (2002) 39 at 47, quoted in M. Sassoli, A. Quintin, ‘Active and Passive Precautions in Air and Missile Warfare’ (n 46) 100. [↑](#footnote-ref-641)
642. AP I, Art. 57 (2) (c). [↑](#footnote-ref-642)
643. Amer, El-Din, ‘The Protection of the Civilian Population’ in N. Ronzitti, G. Venturini, (eds.), *The Law of Air Warfare: Contemporary Issues* *I* (Eleven International Publishing 2006) 28. [↑](#footnote-ref-643)
644. Peter Rowe has raised a similar point in relation to air warfare. See P. Rowe, ‘Kosovo 1999: The Air Campaign – Have the Provisions of Additional Protocol I Withstood the Test?’ 837 *International Review of the Red Cross* (2000). Available at <https://www.icrc.org/en/doc/resources/documents/article/other/57jqct.htm> (retrieved 15 April 2019). [↑](#footnote-ref-644)
645. See S. Oeter, ‘Methods and Means of Combat’ in D. Fleck, (ed.) *The Handbook of international Humanitarian Law in Armed Conflict* (Oxford University Press 2010) 172; A.P.V. Rogers, *Law on the Battlefield* (Manchester University Press 1996) 115; see also Y. Sandoz, C. Swinarski, B. Zimmerman (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 June 1949*, International Committee of the Red Cross (Martinus Nijhoff 1987) at. 2223, according to which ‘giving a warning may be inconvenient when the element of surprise of the attack is a condition of its success’. [↑](#footnote-ref-645)
646. M.N. Schmitt, *Tallinn Manual 1.0* (n 23)171; see also M. Roscini, *Cyber Operations and the Use of Force in International Law* (n 37) 236. [↑](#footnote-ref-646)
647. I. Henderson, *The Contemporary Law of Targeting* (n 15) 189. [↑](#footnote-ref-647)
648. See H.H. Dinniss, *Cyber Warfare and the Laws of War* (n 24)216. [↑](#footnote-ref-648)
649. AP I, Art. 58. [↑](#footnote-ref-649)
650. J-M Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, Vol.1 (ICRC 2005) 67-76. [↑](#footnote-ref-650)
651. C. Greenwood, ‘Customary International Law and the First Geneva Protocol of 1977 in the Gulf Conflict’ in Rowe, P.J. (ed.), *The Gulf War 1990-1991* *in International and English Law* (Routledge, London, 1993) 374. [↑](#footnote-ref-651)
652. H.H. Dinniss, *Cyberwarfare and the Laws of War* (n 24) 218. [↑](#footnote-ref-652)
653. See, in this regard, the account given by Talbot Jensen, E., ‘Cyberwarfare and Precautions against the effects of attacks’ 88 *Texas Law Review* (2010) 1532 at 1542-1545. [↑](#footnote-ref-653)
654. Talbot Jensen, E., ‘Cyberwarfare and Precautions Against the Effects of Attacks’, p. 1555. [↑](#footnote-ref-654)
655. Roscini, M., *Cyber Warfare and International Law*, p. 238. [↑](#footnote-ref-655)
656. Geiss, R., Lahmann, H., ‘Cyber Warfare: applying the principle of distinctions in an interconnected space’ 45 *Israel Law Review* (3), pp.381-399, p. 395. [↑](#footnote-ref-656)
657. Jensen, E.T., *Cyber Attacks and Precautions against the Effects of Attacks*, p.215; Tikk, E., ‘Ten Rules for Cyber Security’ 53(3) *Survival* (2011) 119-132, pp. 126-127. [↑](#footnote-ref-657)
658. Bear in mind, however, that under specific rules of IHL military necessity manifests itself as ‘exceptional military necessity’ and therefore perform a restrictive function, similarly to necessity under IHRL and the *jus ad bellum*. [↑](#footnote-ref-658)