Università
Ca'Foscari
Venezia

Master's Degree

in Comparative International Relations

Final Thesis

Cyber Operations and International Law:
use of force, self-defence and the conduct of hostilities

Supervisor
Ch. Prof. Sara De Vido

Assistant supervisor
Ch. Prof. Arianna Vettorel

Graduand
Delia Bonsignore
853536

Academic Year
2019 / 2020

TABLE OF CONTENTS

LIST OF FIGURES

Abstract

In un mondo sempre più dipendente dalla tecnologia, lo spazio cibernetico si è convertito nella dimensione, seppur artificiale, in cui svolgiamo la maggior parte delle nostre attività. Il progresso tecnologico avvenuto negli ultimi tre decenni ha trasformato il mondo in cui viviamo, rendendolo interconnesso. Nei paesi sviluppati, la maggior parte dei cittadini ha accesso a internet e svolge la maggior parte delle sue attività quotidiane online: dalla comunicazione con gli altri, a pagamenti attraverso conti online, all'acquisto di beni e servizi. Le tecnologie dell'informazione e della comunicazione (TIC) sono largamente usate anche da compagnie pubbliche e private, da piccole e medie imprese a giganti industriali, per il funzionamento delle loro catene produttive. Le TIC sono usate anche dagli ospedali e dal settore sanitario, sia per la ricerca scientifica che per l'erogazione di servizi sanitari ai cittadini. Anche i governi e le pubbliche amministrazioni, insieme alle forze armate e l'intelligence nazionale, fanno largo uso delle tecnologie dell'informazione e della comunicazione. Si evince quindi che lo svolgimento di un gran numero di operazioni si è spostato da un mondo tangibile e naturale a un mondo intangibile e costruito dall'uomo: lo spazio cibernetico. La quinta dimensione, a parte aver apportato grandi vantaggi, ci espone costantemente a nuovi rischi che sono in continua evoluzione, come la cyber criminalità, la cyber frode e il cyber terrorismo. Inoltre, la militarizzazione del cyberspazio ha portato alla creazione di una quinta dimensione della conflittualità, "dove[...] il tipo di armi non militari utilizzate per combattere, così come gli obiettivi presi di mira, rende i sistemi informatici (soprattutto quelli civili) i nuovi centri di gravità da proteggere [...]."[1] Gli Stati più tecnologicamente avanzati e informatizzati sono proprio quelli più soggetti a essere bersaglio di operazioni cyber o di attacchi cyber. Inoltre, il basso costo d'esecuzione di attacchi e operazioni cibernetiche apre la possibilità di utilizzare queste nuove armi non militari a Stati con apparati militari meno competitivi e ad attori non statali.

Anche se la condotta di operazioni cyber non ha portato a tragici scenari finora, eventi recenti hanno dimostrato che le operazioni cibernetiche hanno la capacità di provocare danneggiamento o distruzione fisica di oggetti, oltre che lesioni fisiche a persone o morte. Le

[1] Luigi Martino., "La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale," *Il Mulino - Rivisteweb* Vol.1, (gennaio-aprile 2018): p. 62.

operazioni cibernetiche possono essere utilizzate per spegnere le griglie di distribuzione di energia elettrica, lasciando intere zone senza elettricità; possono essere utilizzate per manipolare le centrifughe degli impianti per il trattamento del combustibile nucleare, mettendo a rischio la popolazione e l'ambiente; possono essere utilizzate per manipolare i sistemi radar per la gestione e il controllo del traffico aereo e di conseguenza causare lo schianto di un aereo, tutto solo con il click di un mouse. Lo spazio cibernetico rende quindi irrilevante la posizione geografica dell'aggressore rispetto al suo bersaglio e accorcia notevolmente la tempistica della condotta di un attacco, dato che è possibile sferrare un attacco da una parte del mondo all'altra in pochi secondi. Inoltre, vista la sua natura intrinseca, la quinta dimensione offre anche moltissime possibilità di anonimato, permettendo all'aggressore di sferrare un attacco con poche possibilità di essere identificato. Per tutte le ragioni sopra elencate, la comunità internazionale è diventata sempre più preoccupata per i rischi che emergono dal cyberspazio: molti Stati hanno incluso tematiche relative alla sicurezza cibernetica nelle loro Strategie per la Sicurezza Nazionale e stanno investendo nel potenziamento delle loro capacità offensive e difensive nella dimensione cibernetica. Inoltre, organizzazioni internazionali come le Nazioni Unite, o regionali come l'Unione Europea, o alleanza militari come la NATO, hanno creato agenzie specializzate in sicurezza cibernetica, con l'obiettivo di rendere la quinta dimensione più sicura.

Molti Stati sono già stati vittime di operazioni cibernetiche presumibilmente condotte da altri Stati. Già nel 1982, l'Unione Sovietica affermò di essere vittima di un attacco cibernetico: una bomba logica - che è un tipo di malware - era stata installata nel sistema di controllo computerizzato di un gasdotto in Siberia e aveva causato un'esplosione. L'Unione Sovietica accusò gli Stati Uniti di aver perpetrato l'attacco, ma la responsabilità degli Stati Uniti non fu mai dimostrata, né tantomeno la veridicità dell'attacco. Nel 2007, l'Estonia fu vittima di attacchi Distributed Denial of Service (DDoS) che durarono per tre settimane e portarono all'arresto dei siti internet del governo, del sistema bancario online e dei siti di informazione. La Russia fu accusata di aver perpetrato gli attacchi cibernetici, visto che questi ultimi furono lanciati in concomitanza con la rimozione di un memoriale di guerra sovietico dal centro storico di Tallinn. Inoltre, il contenuto di molti siti internet fu sostituito con propaganda pro-Russia. Gli attacchi DDoS provocarono lo sconvolgimento del sistema finanziario e di quello delle comunicazioni, ma non provocò il danneggiamento o la distruzione fisica di oggetti, né

lesioni fisiche a persone o morte. Gli attacchi DDoS contro l'Estonia non furono mai attribuiti alla Russia e non furono mai condannati a livello internazionale. Sempre nel 2007, Israele lanciò l'Operazione Orchard contro la Siria. Operazione Orchard comprendeva una fase iniziale, nella quale i sistemi radar per la difesa aerea delle Siria vennero disattivati grazie ad un'operazione cibernetica, e una seconda fase nella quale venne bombardato un reattore nucleare siriano. Nel 2008, l'invasione della Georgia da parte della Russia fu accompagnata da una serie di attacchi DDoS prolungati. Gli attacchi provocarono gli stessi effetti di quelli lanciati l'anno prima contro l'Estonia: arresto dei siti internet del governo e dei sistemi di informazione, contenuto di siti internet sostituito con propaganda anti-Georgia, assenza di danneggiamento o distruzione di oggetti, oltre che assenza di lesioni a persone o morte. Anche questa volta, la responsabilità della Russia per gli attacchi DDoS non fu mai accertata e gli attacchi non furono condannati. Il punto di svolta nella percezione della pericolosità degli attacchi cibernetici arrivò nel 2010 con Stuxnet, che creò un nuovo modello *de facto* per la condotta delle operazioni cibernetiche che gli altri Stati avrebbero potuto seguire. Stuxnet faceva parte dell'Operazione *Olympic Games* lanciata dagli Stati Uniti e Israele contro l'Iran, e viene identificato come il primo esempio di codice militarizzato usato come 'uso della forza'. Il worm fu usato per attaccare l'infrastruttura industriale iraniana con l'obiettivo di manipolare le centrifughe a gas dell'impianto per l'arricchimento dell'uranio di Natanz, che cessarono di funzionare. Escludendo il caso della Siberia del 1982, Stuxnet fu il primo caso in cui un'arma cibernetica risultò in danneggiamento o distruzione fisica, richiamando l'attenzione sul fatto che le operazioni cibernetiche possono effettivamente causare danneggiamento o distruzione fisica e/o lesione di persone o morte.

Allarmati dal fatto che le operazioni cibernetiche possano rappresentare una minaccia alla sicurezza e alla pace nazionale e internazionale, autorità nazionali e organi regionali ed internazionali si sono posti come priorità quella di regolare le operazioni cibernetiche sotto il diritto internazionale e sotto il diritto internazionale umanitario. Viste le caratteristiche peculiari di tale dimensione e la sua notevole velocità di cambiamento, le difficoltà incontrate nel regolamentare le sopracitate operazioni non sono poche. Dalla mancanza di definizioni che demarcano i termini dello spazio cibernetico, a opinioni divergenti che riguardano l'applicazione della legge esistente alle operazioni cibernetiche, la strada per la regolamentazione delle operazioni condotte nel cyberspazio è ancora lunga e tortuosa.

L'elaborato si propone l'obiettivo di analizzare come la *lex lata* riguardante la proibizione della minaccia e dell'uso della forza, il diritto di difesa individuale e collettiva e, nel caso di un conflitto armato, le regole che disciplinano i mezzi e i metodi di combattimento possano essere applicati alle operazioni cibernetiche.

Con questo fine, si analizzeranno i dilemmi interpretativi ancora esistenti riguardo la definizione di 'uso della forza' in riferimento all'Art. 2(4) della Carta delle Nazioni Unite; la definizione di 'attacco armato' in riferimento all'Art. 51 della Carta delle Nazioni Unite; e la nozione di 'attacco' con riferimento al diritto internazionale umanitario. Inoltre, si traccerà una tassonomia delle operazioni cibernetiche conosciute finora, analizzando non solo la loro natura ma anche gli effetti che possono provocare.

In secondo luogo, si argomenterà come e fino a che punto lo *jus ad bellum* e lo *jus in bello* si possono applicare alle operazioni condotte nella dimensione cibernetica. Si proverà a stabilire (1) quando un'operazione cibernetica può essere definita 'uso della forza' e quindi rappresentare una violazione dell'Art. 2(4) della Carta delle Nazioni Unite; (2) quando un'operazione cibernetica può essere definita come 'attacco armato' secondo l'Art. 51 della Carta delle Nazioni Unite e quindi consentire l'uso della forza in legittima difesa individuale o collettiva; (3) quando le operazioni cibernetiche condotte durante un conflitto armato possono considerarsi 'attacco' e quindi essere soggette alle restrizioni e alle proibizioni dettate dal diritto internazionale umanitario.

Per lo sviluppo di questa tesi, l'autore si avvarrà di libri, riviste di settore, periodici cartacei o online, convenzioni e trattati internazionali, risoluzioni delle Nazioni Unite e Direttive dell'Unione Europea, oltre che di documenti prodotti dai governi di alcuni Stati.

List of Abbreviations

AP I	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 8 June 1977
AP II	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
C2	Command and Control
CIHL	Customary International Humanitarian Law
CISA	United States Cyber Security and Infrastructure Security
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operation
CyCon	Annual International Conference on Cyber Conflict
DoD	Department of Defense (United States)
DoS	Denial-of-Service Attack

DDoS	Distributed-Denial-of-Service Attack
EU	European Union
GC I	Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.
GC II	Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949.
GC III	Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949.
GC IV	Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.
IAC	International Armed Conflict
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International Humanitarian Law
IO	Information Operations
IT	Information Technology

LOAC Law of Armed Conflict

NATO North Atlantic Treaty Organization

NATO CCD COE NATO Cooperative Cyber Defence Center of Excellence

NCI National Critical Infrastructure

NIAC Non-International Armed Conflict

NMS-CO National Military Strategy for Cyber Space Operations

NRC National Research Council (United States)

SCADA Supervisory Control and Data Acquisition

SCO Shanghai Cooperation Organization

UNGA United Nations General Assembly

UN GGE United Nations Group of Governmental Experts

UNSC United Nations Security Council

USCYBERCOM United States Cyber Command

WMD Weapons of Mass Destruction

Introduction

The technological advances of the last three decades have reshaped the world we live in in a way that could not have been envisaged by our predecessors. The advent of the internet has created an ever-increasing interconnected world, bringing the world population together and allowing for the sharing of information. The majority of the citizens in developed countries have now access to the Internet and have decided to go online. Citizens, in fact, highly rely on computers, computer systems and networks for the execution of a vast number of their daily activities: from communication with others, to payments made through internet banking accounts, to the purchase of goods and services. Private and public companies, from small and medium enterprises to industrial giants make massive use of computer systems and networks for the functioning of their productive chains and for the delivery of goods and services. Hospitals and the healthcare sector heavily rely on computer systems and networks, both for scientific research and for the delivery of healthcare services. Governments and public administrations make use of computer systems and networks for the management and the delivery of many essential services to their citizens. The armed forces and intelligence units of many States heavily rely on computer systems and networks for the execution of their operations: from espionage, to the mapping of the enemy's territory during an armed conflict, to the development of new weapons and weapon systems to improve their offence and defence capabilities. The execution of a great number of tasks has moved from a tangible natural domain to an intangible man-made domain, that of cyberspace. Cyberspace has been defined as "[t]he global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data."[2] Apart from the enormous advantages brought about by the creation of cyberspace and by the interconnectedness of today's world, we are constantly facing new challenges and threats: from cyber theft to cyber fraud, from cyber activism to cyber terrorism, from cyber criminality to cyber warfare. The more a State relies on computer systems and networks, the more it is vulnerable to threats coming from cyberspace. Furthermore, cyber technologies are

[2] North Atlantic Treaty Organization. *NATO Glossary of Terms and Definitions in English and French. Glossaire OTAN de termes militaires et definitions en englais et française.* NATO Standardization Office (NSO). AAP-06 Edition 2019. p. 37.

relatively cheap to acquire and have become available to States that have weaker military capabilities as well as to non-state actors, changing the dynamics of warfare. In fact, recent events have demonstrated that States can be attacked not only by kinetic means, but also through cyber means. Although no tragic scenario has resulted from the conduct of cyber operations alone, it has already been demonstrated that cyber operations without concurrent kinetic operations can result in the damage or destruction of objects and may even result in injury of persons or loss of human lives. Cyber operations enable actors in the cyber arena to turn off electric power grids leaving entire areas without electricity, manipulate air radar systems causing aircrafts to crash, manipulate the centrifuges of nuclear fuel processing plant causing their malfunction that could lead to tragic consequences both for the environment and for human beings, all of which just with the click of a mouse. Furthermore, cyberspace offers the advantage of making geographical distance irrelevant, since it is possible to launch an attack against a target located in the opposite part of the planet within a few seconds. Attributing a cyber operation to a specific State or actor is very challenging since the cyber realm offers many possibilities for anonymity. For these and many other reasons, States have become always more concerned with cyber security matters and have included them in their National Security Strategies. Furthermore, many States are investing in the strengthening of their cyber defence and offence capabilities. International and Regional Organizations, such as the United Nations, the International Committee of the Red Cross, NATO, the Shanghai Cooperation Organization and the European Union, have created special bodies designed to debate over cyber security-related issues in order to find new ways to make cyberspace more secure.

Several States have already been targets of cyber operations allegedly launched by other States. Already in 1982, the Soviet Union claimed to have been victim of a cyber attack: a logic bomb - which is a kind of cyber weapon that carries a destructive payload- was installed in the computer control system of a gas pipeline in Siberia, causing a major explosion. The attack was allegedly attributed to the United States, but it was never condemned since the responsibility of the US for the attack was never confirmed, nor was the occurrence of the attack itself verified. In 2007, Estonia was victim of distributed denial of service attacks (DDoS) that lasted for three weeks and that brought to the shut down of the government websites together with the banking system and newspapers, among others. The attack was

allegedly attributed to the Russian Federation, given that it followed the removal of a Soviet war memorial that was located in Tallinn and the content of many websites that had been defaced was substituted with pro-Russia propaganda. The DDoS attacks caused the disruption of the economy and of the communication systems, but did not result in physical damage or destruction, nor in the injury or death of persons and it was never condemned internationally. Always in 2007, *Operation Orchard* was launched by Israel against Syria. The military operation entailed a first phase in which a cyber operation disabled the Syrian air defence radars and a second phase in which an airstrike hit a suspected Syrian nuclear reactor. In 2008, Georgia was victim of sustained DDoS attacks that accompanied the Russian invasion of the province of South Ossetia to support the secessionist movement. The DDoS attacks followed similar patterns than those that took place against Estonia the year before: many websites were defaced and their content was substituted with anti-Georgian propaganda, the websites of the government were shut down and the information system was severely disrupted, making it impossible for the Georgian government to disseminate information. Accusations were moved against the Russian Federation, but again, the cyber operations were never condemned since Russia's responsibility was never assessed. Furthermore, the lack of an international legal system that regulates the lawfulness and the conduct of cyber operations makes it really difficult for the victim State to condemn the alleged attacker State and leaves wide range of maneuver for the conduct of such operations. The turning point in the perception of cyber operations was marked by Stuxnet in 2010, that "created a new *de facto* norm for the conduct of cyber engagements other nations [could] follow and imitate."[3] Stuxnet was part of a wider operation called *Olympic Games* launched by the United States and Israel against Iran, and it is considered to be "the first alleged identified instance of weaponised computer code or malware employed as a 'use of force'."[4] The worm was used to attack Iran's industrial infrastructure with the aim of manipulating the gas centrifuges of the Natanz uranium-enrichment facility, that was believed to be used for the development of Iran's nuclear program. If one excludes the case of the gas pipeline in Siberia, Stuxnet was the first case of a cyber weapon used by a State against another State that resulted in physical damage. The malware contained a destructive payload that, apart

[3] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* No. 54, Vol. 4 (2012): p. 108. DOI: 10.1080/00396338.2012.709391

[4] ibid., p. 107.

from self-replicating, manipulated the Supervisory Control and Data Acquisition (SCADA) system of a National Critical Infrastructure (NCI). It worked in two ways: on the one hand, it increased the speed of rotation in the centrifuges, so to cause excessive vibrations; on the other hand, it manipulated the SCADA system that did not record the malfunctions of the plant and sent standard data to the plant operators, who consequently did not notice the malfunction. The worm was able to cause physical damage to the uranium centrifuges.[5] For the first time, a cyber operation alone was able to create physical damage, highlighting the destructive potential of the new cyber tools.

From Stuxnet up to today, many other cyber weapons have been used to achieve military and political goals. Cyber operations have increasingly been used together with kinetic attacks during armed conflicts, or they have been used in times of peace to attack another State without concurrent kinetic operations. The lack of binding norms regulating operations in cyberspace is alarming, mostly because such operations have already demonstrated to have the potential to manifest destructive effects that could seriously endanger national and international security. Furthermore, we are assisting to the militarization of cyberspace: cyber units within the armed forces of several States have been created and cyber operations have been incorporated in their military doctrines. This demonstrates the likelihood that such operations will continue to be used in the future as means and methods of warfare. Therefore, the international community is urging for the adaptation of the existing legal frameworks regulating the resort to force both in times of peace and in times of war to the new domain.

The lack of norms regulating cyber behaviors comes from different reasons: in the first place, boundaries of what is what in the cyber realm have not yet been traced and the international community is struggling in finding agreement over the definitions of 'cyber warfare' and of 'cyber operations' themselves. In the second place, it is still unclear whether the existing legal framework regulating the use of force in times of peace and the resort to armed force during armed conflicts can be applied to the cyber context, and if so, how. The challenges lie in determining if and when a cyber operation amounts to a 'use of force' as intended by Article 2(4) of the United Nations Charter, if and when a cyber operation reaches the threshold of 'armed attack' as intended by Article 51 of the UN Charter, and if and when a cyber operation amounts to 'attack' or to 'resort to armed force' during armed conflicts under International

[5] Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations*, ICRC Expert Meeting, ICRC Reports, Geneva: 14-16 November 2018, p. 54.

Humanitarian Law. In case cyber operations meet the aforementioned thresholds, it is fundamental to determine how these bodies of law apply to the cyber context.

The aim of this final dissertation is precisely that of analysing the existing legal frameworks that prescribe the prohibition of the threat or use of force, the right of self-defence and, in the occurrence of an armed conflict, the rules that regulate the conduct of hostilities in order to determine if such legal frameworks can be applied to cyber operations. To meet this end, in Chapter one the author will bring into light the interpretative quandaries that still surround 1) the notion of 'use of force' under Article 2(4) of the UN Charter; 2) the notion of 'armed attack' under Article 51 of the UN Charter, together with the scope of the right of self-defence and; 3) the classification of a military operation as 'attack' under International Humanitarian Law, together with the rules on the conduct of hostilities. The potential definitions of cyber operation, cyber attack, cyber warfare and cyber weapon will also be discussed. Lastly and fundamental for the regulation of cyber operations under international law, a taxonomy of possible effects resulting from cyber operations will be drawn.

In Chapter two, the findings of Chapter one with regard to the notions of 'use of force' and of 'armed attack' will be applied to the cyber context, in order to explore if and how the rules of the *jus ad bellum* apply to the cyber domain.

In Chapter three, it will be argued whether the rules on the conduct of hostilities set forth by the *jus in bello* apply to cyber operations during pre-existing armed conflicts. It will also be wondered if cyber operations alone can give rise to an armed conflict. After having determined what explained above, the finding of Chapter one with regard to the notion of 'attack' in times of armed conflicts and the legal prohibitions and restrictions that derive from it will be applied to cyber operations reaching the threshold of 'attack'.

CHAPTER 1

The Regulation of the use of force and of warfare under international law

When talking about Cyber operations and International Law, we must distinguish two separate bodies of law that regulate the resort to or the use of (armed) force both in times of peace and in times of war. These bodies of international law are respectively *jus ad bellum* and *jus in bello*. *Jus ad bellum* governs the conditions under which States may resort to the use of (armed) force in times of peace; *jus in bello* governs the conduct of hostilities between belligerents and their relations with third parties in times of war.

The main body of law regulating *jus ad bellum* is the Charter of the United Nations, specifically Article 2 (4), Article 51, and Chapter VII of the aforementioned Charter, and provisions of Customary International Law, formed through state practice and *opinio juris*.

The main body of law governing *jus in bello*, instead, is International Humanitarian Law or the Law of Armed Conflict, which is mostly formed by the Law of The Hague and the Law of Geneva.

The resort to force has been a persistent feature of the global system since the beginning of time. Human beings have waged war on each other to achieve political or strategic goals or to obtain something others possessed. As Arend and Beck explain, with the structuring of societies into political communities, force became one of the most frequent means of interaction among such communities.[6] The establishment of the Modern State during the seventeenth century brought to the proliferation of new varieties of armed conflict. Over the centuries, together with the rapid advances of technology, there was an exponential increase of the destructive potential of warfare. In fact, the level of damage that can be caused by warfare increased up to reach apocalyptic proportions: from the invention of the machine gun, to that of airplanes and submarines, and lastly that of nuclear weapons, human beings are now able to literally destroy humankind.[7] Lastly, the invention of internet has created a new warfare scenario, that of cyberspace. Cyber operations, whose destructive

---

[6] Anthony Clark Arend & Robert J. Beck, *International Law and the use of Force. Beyond the UN Charter paradigm*, (London and New York: Routledge, 1993) p. 2-3.

[7] ibid.

capabilities are still to be seen, have the potential to threaten both national and international security.

In spite of two world wars in the twentieth century alone, that have had tremendous consequences and have resulted in the deaths of over sixty million people, and of the willingness of States to avoid another global confrontation, the use of force has not been abandoned.[8] For this reason, and for the fact that the use of force was not organized under any supranational entity, the international community has tried to regulate it through international conventions and through the creation of international organizations.[9]

As already explained, traditionally the recourse to the use of force was regulated by two separate bodies of international law: the *jus ad bellum* and the *jus in bello*. The *jus ad bellum* applied in times of peace, while the *jus in bello* applied in times of war. Like peace, war was a legal condition, and there was no *status mixtus*. States enjoyed an unlimited right to resort to war, and thus to resort to the use of armed force, as a mean to settle disputes or to achieve political or strategic goals. In order to enter into a relation of belligerency, that is to say, in order to define the act of fighting as 'war', and thus for the Laws of War to be applicable, a formal declaration of war or another formal pronouncement - such as an ultimatum after which States would resort to war - was necessary. Therefore, one of the two or more States parties to the dispute had to explicitly state that it intended to resort to armed force for the purpose of defeating the adversary, so to dictate the conditions for the re-establishment of peace at the end of the war. This behavior is expressed by the term *animus bellandi*[10] and it was codified by the Hague Convention No. III of 1907 relative to the Opening of Hostilities. Article 1 of the Hague III affirms: "The contracting Powers recognize that hostilities between themselves must not commence without previous and explicit

---

[8] ibid., p. 3.

[9] As Arend and Beck explain, there are many reasons for which the use of force has not been abandoned, such as the "inherent aggressiveness of human beings or the sinful nature of humans". Most relevant to this work is, instead, the fact that the use of force in the international realm was not centralized under any authority. This was opposed to the management of force in the domestic realm, in which the use of force is centralized in the modern state and represents one of the pillars of the essence of the modern state itself. The decentralized nature of the use of force in the international realm could be one of the reasons why its use is still in place. See: Anthony Clark Arend & Robert J. Beck, p. 3-4.

[10] Natalino Ronzitti, *Introduzione al Diritto Internazionale,* (Torino*:* G. Giappichelli editore, 2013), p. 471.

warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with the conditional declaration of war."[11]

Although the recourse to war was not restricted, there was already a distinction between 'war' and other uses of force 'short of war', such as reprisals,[12] and self-defence actions.[13] A use of force 'short of war' was defined as a "quick action that did not involve major commitment of forces. It took place in absence of a declaration of war."[14] Such uses of force were regulated by the law of peace. However, prior to the Hague Conventions of 1907, it is estimated that only in 10 out of 117 conflicts there had been a previous formal declaration of war between 1700 and 1870.[15]

One of the first attempts to limit the recourse to war as a mean to settle international disputes is to be found in Art. 1 of the Hague Convention No. I of 1899 concerning the pacific settlement of disputes, that states: "With a view to obviating, as far as possible, recourse to force in relations between States, the Signatory Powers agree to use their best efforts to insure the pacific settlement of international differences."[16]

States Parties to the Convention commit to take all possible measures to peacefully settle their disputes so to prevent, when possible, the resort to armed force in their inter-state relations.[17]

A step further for the restriction of the recourse to force was taken with the adoption of the Covenant of the League of Nations of 1919 - entered into force in 1920. In the event of disputes, under Article 12 of the Covenant of the League of Nations, Member States were

---

[11] *Convention relative to the Opening of Hostilities (Hague III)*, The Hague, 18 October 1907, entered into force on 26 January 1910, Art. 1.

[12] Reprisal: action undertaken by a State to redress an injury suffered during times of peace. This action would normally be considered as a breach of International Law, except when it's undertaken to respond to a previous unlawful act. It does not necessarily involve the use of force. The termination of a treaty, for instance, would be an example of a non-forcible reprisal in response to a violation of a provision of the treaty in question itself. See Arend and Beck, *International Law and the Use of Force*, p. 17-18.

[13] In this period of time, self-defence should not be intended as the contemporary right to self-defence set out by Art. 51 of the UN Charter. Before the entry into force of the UN Charter, an attack as self-defence is interpreted as a protective action aimed at another use of force 'short of war', as Arend and Beck explain. It differs from reprisal in that its purpose is defensive and not retaliatory. See Arend and Beck, *International Law and the Use of Force*, p. 18.

[14] ibid., p. 17.

[15] Christopher Greenwood, "The Concept of War in Modern International Law," *International and Comparative Law Quarterly* Vo. 36, No. 2 (1987): p. 285.

[16] *Convention for the Pacific Settlement of International Disputes (Hague, I), The Hague, 29 July 1899*, entered into force on 4 September 1900, Art. 1.

[17] Natalino Ronzitti, *Introduzione al Diritto Internazionale,* p. 412.

obliged to "submit the matter either to arbitration or judicial settlement or to enquiry by the [League] Council, and they agree[d] in no case to resort to war until three months after the award by the arbitrators or the judicial decision, or the report by the Council. [...]."[18] Moreover, if there were the unanimous adoption of an arbitral or court decision,[19] or the adoption of a report made by the Council of the League,[20] the parties to the dispute were obliged to abstain from the resort to war against any other party to the dispute which was complying with the arbitral or court decision, or with the recommendations made in the report of the Council. If one party to the dispute was not abiding to the arbitral or court decision, or to the recommendations set out by the report of the Council, the other party or parties could wage war against the first *only* three month after the award by the arbitrators or the judicial decision or the report of the Council.[21]

Article 16 provided commercial and financial sanctions to the Member States resorting to war without having previously taken the steps for the peaceful settlement of the dispute agreed in Article 12.

The system created by the League of Nations imposed significant restrictions to the recourse to war, but war itself was not outlawed. In fact, under Article 15, if the arbitration body, the court or the Council failed to unanimously adopt a decision, Member States could take the actions they deemed necessary to solve the dispute. In other words, in this case, Member States were not obliged to refrain from the use of force or from the possibility to wage war. Moreover, the League did not apply any restriction on uses of force 'short of war'.

The Kellogg-Briand Pact of 1928, also called General Treaty for Renunciation of War as an Instrument of National Policy, sets forth the abandonment of the resort to war as an instrument of national policy and strongly condemns the recourse to it as a mean to settle international controversies. Article 2 of the Pact clearly states that disputes must be settled by peaceful means only.[22] Hence, unlike the Covenant of the League of Nations, which allowed the recourse to war in the circumstances explained above, the Kellogg-Briand Pact outlawed

---

[18] *Covenant of the League of Nations*, Art. 12.

[19] ibid., Art. 13.

[20] ibid., Art. 15.

[21] ibid., Art. 12.

[22] " [...] the settlement or solution of all disputes or conflicts of whatever nature or of whatever origin they may be, which may arise among them, shall never be sought except by pacific means.", in *General Treaty for Renunciation of War as an Instrument of National Policy*, Paris, 27 August 1929, entered into force on 25 July 1929, Art. 2.

the resort to war. The only exceptions to this proscription that were generally accepted by States were the resort to war that had been previously authorized by the League of Nations, and self-defence.

Two main problems remained unsettled after the entry into force of the Pact in 1929: firstly, the Pact did not impose any restriction on the uses of force below the threshold of war; secondly, the Pact did not define what actions short of war could justify the recourse to self-defence, so its interpretation remained unclear.

The uses of force below the threshold of war and the actions 'short of war' that could trigger the applicability of self-defence will be set out by the United Nations Charter in 1945. After the end of the Second World War and the clear failure of the League of Nations, Allied Powers were convinced that another effort had to be made to create an international organization in charge of the management of international conflicts. More significantly, Allied Powers felt the urgency to retain the governance of the use of force under one single international authority. The centralization of the use of force would have guaranteed the limitation of its usage by single States.

Furthermore, only after the entry into force of the four Geneva Conventions of 1949 the Laws of War, that will be called International Humanitarian Law, will become applicable to other types of armed conflicts not strictly classifiable within the traditional meaning of war.

1. The use of force under the UN Charter regime

The law on the use of force is one of the most controversial areas of international law and there is still disagreement over the interpretation of its fundamental provisions, especially with regard to the threshold required for an action to be classified as threat or use of force, and in such case, as to what is the threshold required for the use of force to be considered as an armed attack triggering the application of the right of self-defence.

The Charter of the United Nations is the main source of international law regarding the use of force, as it explicitly prohibits both the threat of force and the use of force in Article 2(4):

> "All Members shall refrain in their international relations from the threat or use of force against the

territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[23]

The United Nations was created as a response to the cruelty of World War II, so to "save succeeding generations from the scourge of war", as stated in the Preamble of its Charter. The founding of the international organization itself aimed at avoiding the outbreak of future wars, setting out the maintenance of international peace and security as one of its three pillars,[24] of which the United Nations Security Council (UNSC) is in charge.

The UN Charter provides methods for the pacific resolution of disputes in Chapter VI, and when such methods prove to be insufficient, it provides a set of enforcement actions that can be taken under the guidance of the UNSC. The Charter not only aims to prohibit the use of force, but also to centralize its control in the Security Council, acting under Chapter VII of the same Charter.

The only two exceptions to the prohibition of the use of force that still have major significance are the uses of force authorized by the Security Council under Chapter VII and the right to individual or collective self-defence under Article 51.

As far as Chapter VII of the UN Charter is concerned, the Security Council has the authority to "determine the existence of any threat to peace, breach of the peace, or act of aggression"[25] and it "should respond to threats to the peace, breach of the peace, and acts of aggression, if necessary through its own standing army."[26] The UNSC, in order to respond to threats to peace, breaches of the peace or acts of aggression can make recommendations or, under Article 41, impose measures not involving the use of force on an offending state, such as the total or partial interruption of economic relations. Should these measure be found to be insufficient to halt the threat to or breach of the peace or act of aggression, the Security Council can take military actions by land, air or sea under Article 42 of the Charter. The UN armed force, envisaged by Article 43, was never created, leaving it to States to gather in the so-called 'Coalition of the willing', through which such States can use force in major enforcement operations under the authorization of the United Nations Security Council, when

---

[23] *UN Charter*, Art. 2(4).

[24] ibid., Art. 1.

[25] ibid., Art. 39.

[26] Christine Gray, "The use of force and the international legal order," in *International Law*, ed. Malcolm D. Evans (New York: Oxford University Press, 2018) (fifth edition): p. 602.

the organization founds itself devoid of the resources necessary to undertake the aforementioned enforcement operations.

Article 51, instead, concerns the inherent right of self-defence, under which a victim State can lawfully resort to the use of force until the United Nations Security Council is ready to take actions to restore international peace and security. Article 51 states: "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, until the Security Council has taken the measures necessary to maintain international peace and security [...]."

This rule of international law is accepted to be also customary international law. Therefore, the use of force is lawful only in the case in which a Member state is victim of an armed attack launched by a *de jure* or or a *de facto* organ of another State.

Both Article 2 (4) and Article 51 of the UN Charter raise questions with regard to their specific interpretation, since they do not define what is meant for threat or use of force, and what is meant for uses of force that reach the threshold of armed attack triggering the right of self-defence. The UN General Assembly (UNGA) attempted to solve such interpretation quandaries by passing a set of resolutions, as the *Declaration on Friendly Relations*[27] and the *Definition of Aggression*.[28] Judgements of the International Court of Justice, such as the *Nicaragua* case,[29] and State practice further helped to solve interpretative ambiguities.

The first question that has to be addressed is what exactly is a 'threat or use of force'. Some, especially developed countries, claimed that the interpretation of 'threat or use of force' should be limited to military force or armed force only, while others, especially developing countries, felt the need to include in the interpretation also diplomatic or economic measures that could severely affect the stability of a State. Nowadays, the debate over the meaning of threat or use of force also addresses the possibility of classifying a cyber operation as use of force.

---

[27] *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (A/8082)*, A/RES/2625 (XXV) (24 October 1970).

[28] *Definition of Aggression*, A/RES/3314 (XXIX) (14 December 1974).

[29] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* (Merits) *ICJ Reports 1986*

1.1 The meaning of 'threat or use of force'

As for the meaning of 'threat of force', the International Court of Justice (ICJ) limited itself in stating that "a threat to force is unlawful where the actual use of the force threatened would itself be unlawful"[30] in its Advisory Opinion on the *Legality of Nuclear Weapons*. The Court drew the distinction between the mere ownership of nuclear weapons and nuclear dissuasion. Whereas the mere ownership of nuclear weapons does not represent in itself a threat of force, nuclear dissuasion finds its roots in the threat of the use of nuclear weapons, since the State that is in possession of such weapons is ready to use them in response to a nuclear attack. Knowing that the nuclear weapon will be used against it, the aggressor abstains from using nuclear weapons in the first place.

Despite this distinction, the Court did not condemn nuclear dissuasion; in fact, it affirmed that the lawfulness of nuclear dissuasion is proportional to the lawfulness of the actual use of nuclear force threatened. If the use of nuclear force in question is lawful (e.g. use of force as self-defence), so will be nuclear dissuasion.[31]

Debate arose over whether the establishment of considerable armaments by a State (armaments race) could be regarded as a threat of force for neighboring States. The ICJ excluded such possibility. In the *Nicaragua v. United States of America* case, the Court, in agreement with Customary International Law, affirmed that there is no limit for the level of armament of a State.[32] Restrictions in this sense can arise only through treaty law, especially through treaties related to arms limitation or disarmament.

An example of a threat of force could be an *ultimatum*: after the expiration of the ultimatum, if the conditions previously imposed were not respected, the State giving the ultimatum would resort to the use of force.[33]

As for the definition of 'use of force', the ICJ sets out the general doctrine in this area, especially through the *Nicaragua* judgement. In this case, in order to determine when an act can be considered a use of force, the ICJ distinguished between the 'most grave' forms of the

---

[30] Christine Gray, "The use of force and the international legal order", p. 604.

[31] Natalino Ronzitti, *Introduzione al Diritto Internazionale,* p. 415-416.

[32] See *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* (Merits)*, ICJ Reports 1986*, 135, par. 269.

[33] Natalino Ronzitti, *Introduzione al Diritto Internazionale,* p. 415.

use of force - classified as those amounting to armed attack for the purposes of the law of self-defence-, and other 'less grave' forms. Instead of looking only at the nature of the action, the Court focused on the 'scale and effects' of the action, that of course *has* to be conducted by or be otherwise attributable to a State. The " 'scale and effects' is a shorthand term that captures the quantitative and qualitative factors to be analysed in determining when [an action] amounts to a use of force."[34] In short, what was found was that "uses of force need not involve a State's direct use of armed force, and [that] all armed attacks are uses of force."[35] This statement still leaves open the question as to what actions short of armed attack actually constitute a 'use of force'. In the *Nicaragua* case, the Court found that the arming and the training of the *contras* by the United States was to be considered a 'use of force'. This provides an example of what the definition of use of force may entail, even though force is not directly used by the State committing the violation. The supplying of funds to the *contras*, however, was not a use of force in itself, even though it was a breach of the principle of non-intervention in other States' internal affairs.

The possibility for economic coercion to be considered as use of force has long been debated, and although prohibited by some UNGA Resolutions, such as the aforementioned *Declaration on Friendly Relations*, it was not found to meet the criteria required in order to be classified as use of force.

1.2 The meaning of territorial integrity, political independence and the purposes of the United Nations

The second part of Article 2(4) of the UN Charter has been in the spotlight of many debates, and it has been a reason of disagreement among many States. Since Article 2(4) prohibits the threat or use of force "against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations", does it allow the use of force if the aim of its use is not to overthrow the government or seize its territory, provided that the action itself is not inconsistent with the purposes of the United

---

[34] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, (New York: Cambridge University Press, 2017), p. 331.

[35] ibid., p. 333

Nations?[36] Or is it, on the contrary, a strict prohibition on all uses of force? Moreover, can there be a use of force that does not harm the political independence or territorial integrity of a State?

Debates have focused on whether the use of force to rescue one's nationals, to promote democracy, or to further self-determination could be consistent with Article 2(4). Humanitarian Intervention was also discussed in the light of NATO's forcible intervention in Kosovo in 1999.

Some argued that the prohibition of Art. 2(4) had to be interpreted as limited to the context of the Charter; this narrow interpretation provided that States could lawfully use force for purposes compatible with the United Nations, such as the rescue of nationals abroad, as argued by Israel after its operation to rescue its nationals on a hijacked plane from Entebbe (Uganda) in 1976, and by the USA in its operation in Grenada in 1983. A part from these cases, no other State justified its actions by applying a narrow interpretation of Art. 2(4). If anything, States tend to justify their actions as self-defence instead of relying on the compatibility of their actions with Art. 2(4).

The lawfulness of the use of force in pursuit of self-determination was also a matter of discussion, but nowadays it encounters no support if taken outside the context of decolonization or illegal occupation.[37] The use of force is not considered lawful in pursuit of democracy either: the fact that, in exceptional cases, the United Nations may have the power to authorize the use of force to restore a democratic government should not be extrapolated and transformed into a right of unilateral intervention by States.[38]

The aforementioned are just some examples of when an action can be identified as a breach to the prohibition of the use of force. Unfortunately, clearer definitions of what a use of force is were not deliberately given neither by the UN General Assembly nor by the International Court of Justice. The ICJ, in fact, has regarded the provisions of the UN Charter as dynamic, and thus capable of changing over time with state practice.[39]

---

[36] Christine Gray, *International Law and the Use of Force*, (New York: Oxford University Press, 2004), p. 29.

[37] See ibid., p. 52- 58.

[38] Christine Gray, "The use of force and the international legal order", p. 606.

[39] Christine Gray, *International Law and the Use of Force*, p. 7.

1.3 The use of force in international relations

The scope of the prohibition of the use of force contained in Art. 2(4) of the UN Charter does not embrace every threat or use of force. It concerns only the uses of force exercised by States in their *international relations*. The use of force exercised beyond one's territorial borders is certainly in the scope of the prohibition, both in the case of the territory of another State and in the case of international territories, as high seas or the international airspace. The use of force by State A in its own territory against the organs or properties of State B lawfully located in the territory of State A falls within the scope of the provision, as well as the use of force against State B's troops lawfully allocated in the territory of State A. Doubts remain over the use of force against diplomatic representatives or against a diplomatic mission.

The prohibition does not apply to those uses of force made by a State in its own territory against its own people; such actions would be a breach of other principles of International Law, but they would not be considered as a violation of Art. 2(4) of the UN Charter.[40]

The fact that Article 2(4) prohibits the use of force by States in their international relations was used to justify the use of force for the seizure of territories under the control of another State. In 1982 Argentina invaded the Falkland Islands claiming its sovereignty over the islands, that had been seized by the UK in 1833; in 1990 Iraq invaded Kuwait claiming that it had pre-colonial title over Kuwait's territory. In both cases, the States affirmed not to be violating Article 2(4) since the territories in question had previously been under their sovereignty. These actions, however, were strongly condemned by the international community.

The interpretation of Art. 2(4) with regard to its reference to 'international relations' has been challenged also by the categorization of conflicts. Is a situation that of an inter-State conflict or is it an internal conflict governed by different rules? The categorization of conflicts is fundamental for the applicability of the law, and it has brought disagreement in various cases, such as the Vietnam and Korean Wars.

It is acknowledged that the prohibition of the use of force is clearly directed at inter-State conflicts, but since its entry into force, the most common uses of force have taken place

[40] Natalino Ronzitti, *Introduzione al Diritto Internazionale,* p. 416-417.

during civil wars, "sometimes purely internal, sometimes fueled by outside involvement."[41] In order to deal with foreign State's involvement in civil wars, the UN General Assembly has developed resolutions "which elaborate on the Charter provisions on the use of force and complement the prohibitions of forcible intervention in civil conflicts,"[42] such as the *Friendly Relations Declaration* of 1970. Moreover, in the *Nicaragua* case, the ICJ was forced to address the questions arising from foreign intervention in a civil conflict that, depending upon the interpretation of the facts, could be considered as a 'mixed conflict'. Since the Charter provisions on the use of force do not address types of conflicts other than international ones, the Court attempted to apply the logic of the Charter restrictions to civil wars and mixed civil-international conflicts as well. The outcome of this attempt was the formulation of 'norms' of intervention.[43]

The progresses made by information technology (IT) and its wide use in the military context have lead to the question of whether the launching of cyber operations against a State could be considered a breach of Art. 2(4) of the Charter. In absence of an international agreement or other international binding document on the regulation of cyber operations, the applicability of Art. 2(4) to cyber operations is just a supposition. It is known that cyber operations have been used during armed conflicts, so to render ineffective the defenses of the adversary. So far, their use would not fall under the scope of Art. 2(4), but mostly under the regulation of the means and methods of warfare. In case cyber operations would be used to manipulate the financial system of a State, such conduct could be thought to breach the prohibition of intervention, for instance. Cyber operations that could constitute a breach of the prohibition of the use of force could be the bombing of the territorial state with its own missiles or with the missiles of a third State, by manipulating their launch system. Other examples could be the service denial of computers that control the water reserves of a country or the dams of a country so to cause the death of hundreds of people. The cyber context will be analyzed in Chapter 2.

---

[41] Christine Gray, "The use of force and the international legal order", p. 609.

[42] ibid.

[43] Anthony Clark Arend & Robert J. Beck, *International Law and the use of Force. Beyond the UN Charter paradigm*, p. 80.

2. Self-defence and the notion of 'armed attack'

For the purpose of understanding when self-defence is allowed under Article 51 of the UN Charter, the definition of armed attack must first be given. The term is used in the two previously mentioned bodies of law: the *jus ad bellum* and the *jus in bello*. As already explained, *jus ad bellum* governs the resort to force by States in times of peace. In this context, an armed attack is *conditio sine qua non* to lawfully use force in self-defence, under Article 51 of the UN Charter and according to Customary International Law. *Jus in bello*, or International Humanitarian Law is, instead, a body of law that contains prohibitions and restrictions with regard to the use of armed force in times of war. It regulates the conduct of hostilities by safeguarding, among others, the civilian population and cultural sites. In this context, the term armed attack refers to a type of military operation to which the restrictions and prohibitions of International Humanitarian Law apply.

2.1 The scope of the right of self-defence

As already explained, one of the main exceptions to the prohibition of the use of force set out by Article 2(4) of the UN Charter is Article 51 on the right of self-defence. The Article provides that:

> "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, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

Scholars and States disagree over the narrow or wide interpretation of the Article. The debate revolves around the scope of the provision: is Article 51 an exhaustive description of the right of self-defence or is there a wider right of self-defence expressed by customary international law whose scope goes beyond the right to respond to an armed attack?

Those in support of a wider interpretation of Article 51 argue that the Article explicitly states that self-defence is an 'inherent right' and that for such reason it should be

interpreted as preserving a wider customary law right of self-defence, allowing self-defence other than against an armed attack. According to them, the right of self-defence includes also the protection of nationals abroad and the right of pre-emptive self-defence, for instance.[44]

Those in support of a narrow interpretation of Article 51 argue that it explicitly and purposely imposes restrictions on the right of self-defence by limiting it as a response to an armed attack only. Accepting a wider interpretation of the provision would deprive it of its main purpose: the *limitation* of the right of self-defence, as Gray explains. In addition, the interpretation of the right of self-defence as a wider right would contradict both the willingness of the United Nations to limit the use of force, and one of its three pillars, namely the maintenance of international peace and security.

During the drafting of the Charter in San Francisco, delegates agreed that force was too destructive to be considered as a possible mean to pursue political goals or even to right a past 'wrong'. In their perspective, "force was to be used only for 'value conservation', for the preservation of existing political and territorial status quo, either through the exercise of self-defence or as determined by the Security Council."[45] As Arend and Beck explain, the value choice made by the delegates of San Francisco with regard to the use of force was that the maintenance of peace was to be preferred to the pursuit of justice. Justice was undoubtedly to be pursued, but not at the expenses of peace. In fact, they believed that using force to promote justice would have harmed the international community more than living with a particular injustice.

The reasoning of the delegates of San Francisco provides a clearer framework on how Article 51 should be interpreted. However, the growing preference for 'justice' over 'peace' has challenged the application of the provision. Some States have claimed that the use of force to promote self-determination, to correct past 'injustices', and to resort to 'just' reprisals had to be justified.[46]

---

[44] Christine Gray, "The use of force and the international legal order", p. 611.

[45] ibid., p. 34.

[46] For more, see Anthony Clark Arend & Robert J. Beck, "The United Nations Charter framework for the resort to force", in *International Law and the use of Force*. *Beyond the UN Charter paradigm*, (London and New York: Routledge, 1993).

2.1.1 Necessity and Proportionality

Notwithstanding the debate over the interpretation of the scope of Art. 51, there is broad agreement about the fact that self-defence must be necessary and proportionate. These requirements are not mentioned in the UN Charter, but they have become part of customary international law. The response to an armed attack in self-defence must be "necessary to recover territory or repeal and attack on a State's forces and which is proportionate to this end."[47] The fact that necessity and proportionality constitute restrictions applicable to all cases of self-defence, both individual and collective, has been affirmed by the ICJ in the *Nicaragua* case, in the *Oil Platforms* case and in the Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*.

For the principle of necessity, a use of force in response to an armed attack is lawful only when non-forceful measures, such as diplomatic or economic sanctions, prove to be insufficient to repeal or halt the armed attack the victim State is subjected to. The principle of proportionality is strictly connected to that of necessity, and it addresses how much force is proportionate to achieve the victime State's goal of responding to an armed attack, when a forceful response is deemed necessary for that end. Therefore, necessity and proportionality implicitly express that self-defence should not be punitive or retaliatory, but that it should be used only for the purpose of stopping or repelling an armed attack. However, this does not imply that the defending State has to comply with certain criteria when engaging in self-defence actions, such as the limitation of the response to its own territory, or the usage of the same weapons, or the same number of armed forces as the attacking State. Proportionality, indeed, aims at limiting the scale, scope, intensity and duration of the use of force in self-defence to that necessary for the halting of the situation that triggered the right to forcefully respond in self-defence in the first place.

There are no specific boundaries or descriptions of the requirements of necessity and proportionality; they depend, indeed, on the facts of each particular case. Both in the *Nicaragua* and in the *Oil Platforms* cases, the ICJ used such requirements as marginal considerations in the logic of its judgments because, in both cases, the use of force by the United States had already been held not to qualify as lawful self-defence since the US had not

[47] Christine Gray, "The use of force and the international legal order", p. 612.

been victim of an armed attack. In these two cases, the limitations of necessity and proportionality only confirmed the illegality of US actions. However, these limitations are often taken into account in State practice and used to determine the legality of a particular action. As Gray explains, "[t]hey constitute a minimum test by which to determine that a use of force does not constitute self-defence."[48] In fact, in Security Council debates, States have been able to avoid getting involved into doctrinal arguments as to whether the right of self-defence is a wide or narrow right, by simply saying that a particular use of force was neither necessary nor proportionate and thus illegal.

2.1.2 The meaning of 'armed attack'

As explained in the paragraph above, the use of force is considered lawful when a State is exercising its right of self-defence against an armed attack. However, Article 51 does not contain any definition describing what actions can be considered as an 'armed attack'.

During the San Francisco Conference, the phrase 'armed attack' was not defined, probably because it was regarded as sufficiently clear and self-evident. However, it soon became clear that its interpretation was not so straightforward. Some argued that, for an attack to trigger Art. 51, it "should be of a serious nature that threatens the inviolability of the attacked State."[49]Others claimed instead that even a single gunshot fired by an armed soldier across the border could qualify as armed attack. Moreover, questions arose as to whether the term 'armed attack' in Article 51 precluded the possibility of exercising the right of self-defence against illegal uses of force that did not reach the threshold of armed attack.

Since then, the international community has discussed what actions can actually be considered as reaching the threshold of armed attack so to trigger the application of Article 51 of the UN Charter. Scholars have come to different conclusions with regard to the narrow or wide interpretation of the notion of 'armed attack'. Christine Gray explains that "[t]he most straightforward type of armed attack is that by a *regular army* of one State against the

---

[48] Christine Gray, *International Law and the Use of Force*, p. 124.

[49] Stanimir A. Alexandrov, *Self-Defense Against the Use of Force in International Law*, (The Hague: Kluwer Law International, 1996), p. 97.

territory or against the land, sea, or air forces of another."[50] However, its meaning evolves together with customary international law.

2.1.2.1 The meaning of 'armed'

The evolution of warfare and the emergence of new weapons have challenged the interpretation of the adjective 'armed' when it applies to attacks in the context of the right of self-defence. The challenge lies in establishing if the type of arm employed for an attack is relevant for the classification of the action as armed attack, and if so, what types of arms can be considered as means to deploy an armed attack under the scope of Art. 51 of the UN Charter.

The International Court of Justice, in its *Nuclear Advisory Opinion*, stated that both Art. 2(4) and 51 of the Charter apply to any use of force, regardless of the weapons employed. This statement is a reflection of customary international law.

In the past two decades, but mostly after the malicious cyber operations conducted from 2008 onward, there has been a growing debate over the consideration of certain cyber operations as armed attacks. There is still disagreement on the necessity for an attack to cause physical harm to people or property in order to be considered as to have reached the threshold of an armed attack. The matter will be discussed in the following Chapter.

Going back to the definition of 'armed', in the first place, it is important to point out that the adjective " 'armed' is not to be equated with the term 'force' in the sense of Article 2(4)."[51] The ICJ identified this normative "gap" in the *Nicaragua* Judgement when it affirmed that not all uses of force are armed attacks, whist all armed attacks are uses of force. In order to demarcate the difference between use of force and armed attack, the Court distinguished between the 'most grave forms' of the use of force and 'other less grave forms'. A 'most grave form' of use of force classifiable as armed attack, implies "[...] an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (i.e.

---

[50] Christine Gray, "The use of force and the international legal order", p. 612.

[51] Michael N. Schmitt, ""Attack" as a Term of Art in International Law: The Cyber Operations Context", in *2012 4th International Conference on Cyber Conflict*, eds. C. Czosseck, R. Ottis, K. Ziolkowski (Tallinn: NATO CCD COE Publications, 2012,) p. 286.

scale) which have as their consequences (i.e. effects) the infliction of substantial destruction upon important elements of the target State, [...]"[52] as well as the loss of lives.

The important elements of the target State are thought to be its economic and security infrastructure, together with its people; the destruction of elements of its governmental authority, as its political independence, for instance; and the damage or deprivation of its territory.[53] In short, an armed attack that triggers the applicability of the right of self-defence is one that causes "a considerable loss of life and an extensive destruction of property."[54]

A 'less grave form' of use of force, as affirmed by the ICJ, would be the supply of weapons or the provision of logistical support to rebels in another State, for instance.

In the second place, it is important to note that, as Schmitt explains, "Article 51 adopts an "act-based" threshold using a specific type of action (armed attack) rather than one based on particular consequences."[55] This approach fit the needs of the international community in 1945, when the possible uses of force reaching the threshold of 'armed attack' were carried out through classical military means.

The drafters of the UN Charter, when thinking about the meaning of 'armed attack', considered the standard weaponry of the Second World War, indeed. However, the evolution of weapons and of warfare challenged the validity of this approach, that is thought to be unsuitable nowadays, especially with the advent of cyber operations. The conventional view of the drafters had not changed when the discussions for the *Definition of Aggression* began in 1956, occasion in which the definition of 'armed attack' was taken into consideration as well.

In 1961 Brownie proposed the consideration of bacteriological, biological, and chemical weapons as means to launch an armed attack, as their consequences can be destructive to persons and objects as the ones caused by kinetic weapons. Brownie moved the spotlight on the consequences caused by the use of other non-conventional weapons comparable to the consequences caused by the use of kinetic weapons, instead of focusing on the weapons used

---

[52] Karl Zemanek, "Armed Attack" in *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law*, eds. Frauke Lachenmann and Rüdiger Wolfrum, (New York: The Max Planck Foundation for International Peace and the Rule of Law and Oxford University Press 2017, 2017) p. 28.

[53] ibid.

[54] ibid.

[55] Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, p. 287.

stricto sensu. In fact, it is argued that the act-based approach used for the interpretation of the adjective 'armed' should be substituted by an effect-based approach, due to the fact the new century has brought to the creation of weapons that do not fall under the notion of traditional weapons in the kinetic sense, but that are able to cause dire consequences that can be as severe as the ones provoked by conventional weapons and conventional military operations.

Finally, the traditional meaning of the adjective 'armed' is related to the carrying or using of weapons, suggesting that the *consequences* implied are those naturally related to the use of weapons, such as death or injury to persons, or destruction or damage to objects. No agreement has been reached so far over what degree of harm is necessary to qualify the consequences of certain uses of force as sufficiently severe to reach the threshold of armed attack, but if the effect-based approach was to be used, a new set of operations could potentially fall under the notion of armed attack in the meaning of Art. 51 of the UN Charter. Although the ICJ has stated in its *Nuclear Advisory Opinion* that the type of weapon used is irrelevant to the application of Articles 2(4) and 51, there is still no consensus with regard to the classification of cyber operations as armed attacks.

2.1.2.2 "By a regular army"

Once again, the ICJ judgment on the *Nicaragua* case provides the guidelines for interpreting the provisions of the UN Charter. The Court relied on the *Definition of Aggression* to support its view and stated that:

> "an armed attack must be understood as including the sending in or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to an actual armed attack, or its substantial involvement therein'."[56]

Thus, according to the ICJ, an armed attack does not have to be conducted necessarily by the *regular forces* of a State. The Court found that attacks carried out by mercenaries, irregular forces or groups can be attributable to a State depending on its degree of involvement with the attackers. In fact, in the *Nicaragua* case, what the Court evaluated was the degree of involvement of the United States in the actions carried out by the *contras*. Moreover, in the Court's opinion, the assistance to rebels in the form of logistical support or provision of

[56] ibid.

weapons *alone* did not amount to armed attack; nevertheless, these types of assistance could be classified as unlawful intervention.[57]

The narrow definition of 'armed attack', that initially included only armed attacks carried out 'by a regular army' was challenged again after 2001: since the 9/11 terrorist attacks by Al-Qaeda against the Pentagon and the World Trade Center, the notion of armed attack has come to include the use of force by terrorist organizations, even when their actions lack of State involvement, overcoming the new boundaries of the definition that had been set out by the ICJ in the *Nicaragua* case. For what concerns the 9/11 attacks, however, the Security Council did not explicitly state that the terrorist attack amounted to armed attack, and it preferred to characterize it as 'threat to peace'. In any case, the UNSC affirmed the applicability of the right of self-defence in the preambles to Resolutions 1368 and 1373, strongly condemning the terrorist attacks.[58]

2.2 Other Controversies over the scope of Article 51

Apart from what has been said so far, the debate over an extensive or restrictive interpretation of Article 51 has arisen further controversies. Those in support for an extensive interpretation of the right of self- defence have argued for a right to protect nationals abroad and for a right of anticipatory self-defence. Their standpoint has been stimulated by the advance of new technologies and weapons, such as nuclear weapons, and historical events that have presented new challenges for/to international and national security, such as large-scale terrorist attacks. In addition, the value of the right of collective self-defence itself has been questioned, especially with regard to its effectiveness in representing a valuable safeguard for smaller states.

[57] ibid.

[58] ibid.

2.2.1 The Protections of nationals abroad

As State practice shows, some States have justified their use of force in foreign countries as a mean to protect their nationals abroad. Such States viewed their intervention as an extension of their right of self-defence. Article 51 of the UN Charter, in fact, does not specify if the right of self-defence can be exercised *only* if the armed attack occurs in State A's territory, or if the right can be exercised also in State B's territory if State A's citizens are in danger or attacked. In other words, can State A lawfully use force under Article 51 in State B's territory without its expressed consent if State A's citizens located in State B's territory are subject to imminent threat of injury? A scenario of a possible threat of injury for State A's citizens in State B's territory is the outbreak of internal upheavals in State B's territory, for instance.

This right has been asserted mostly by developed States, especially by the United Kingdom, as in Suez in 1956; by Israel, in Entebbe in 1976 for instance; and by the United States, as in the case of Grenada in 1983 and Panama in 1989. The intervention of the United Kingdom in Suez dictated the general doctrine for those in support of a wider interpretation of the right of self-defence as including the protection of nationals abroad. In this case, in the UK's opinion, the conditions for a lawful use of force in a foreign country to protect one's nationals were: 1) the existence of an imminent threat of injury to nationals; 2) the inability of the territorial sovereign State B to protect the nationals of State A located in State B's territory; 3) the limitation of the operation to the protection of nationals *only*.[59] In most of the cases, what was observed was that the operations to rescue one's nationals abroad were not limited to such purpose, but served wider objectives, mainly political ones - such as the installation of a new government in State B's territory as in the case of Grenada, for instance.

A quite recent example in which a State justified its use of force as right of self-defence for the protection of nationals abroad was the use of force by Russia against Georgia in the province of South Ossetia in 2008. In this case, Russia claimed that its intervention in the Georgian province was lawful under the right of self-defence because many ethnic Ossetians held Russian passports. However, when the conflict spread to the province of Abkhazia, that was fighting for independence as well, Russia sent its troops to both the Georgian provinces,

[59] Christine Gray, *International Law and the Use of Force*, p. 128.

forcing Georgian troops to withdraw and helping the provinces achieve political independence. Western States judged Russian actions as unlawful since they were not limited to the protection of Russian nationals, but aimed at the dismantlement of Georgia. The Russian Federation used the same justification for its intervention in Crimea in 2013-2014.

It can be observed that, in most cases - excluding the aforementioned intervention in Entebbe by Israel for instance-, the intervention is not limited to the protection of nationals abroad. Developing States, in fact, are more doubtful with regard to the existence of this right since, as in the case of Georgia, it is often a pretext for achieving far-reaching political goals rather than the mere protection of nationals.

There is still doctrinal divide over the legality of intervention for the protection of nationals abroad, but State practice has shown that there is no overall support for the interpretation of the Charter as allowing forcible protection of nationals abroad.

2.2.2 Anticipatory and pre-emptive self-defence

Other controversies have arisen with regard to whether an imminent threat is sufficient to create an immediate right to resort to force in self-defence. In other words, is the right of self-defence limited to the exercise of the use of force only *after* an armed attack has occurred, or is there a wider right to anticipate an imminent attack, when the imminence of the attack is recognized by the victim-to-be State?

As Alexandrov argues, a narrow interpretation of Article 51 of the UN Charter would bring to the conclusion that the right of self-defence can be exercised only *after* an armed attack has actually occurred by one State against another State. In the words of Alexandrov, Article 51's "*if* an armed attack *occurs*"[60] should thus be interpreted as "*after* an armed attack *has occurred*". Thus, anticipatory self-defence would be unlawful in spite of the "imminent and grave danger of aggression."[61] Furthermore, Christine Gray argues that an anticipatory attack in self-defence "involves a risk of escalation in that the State may mistake the intentions of

[60] *UN Charter*, Art. 51.

[61] Stanimir A. Alexandrov, p. 99.

the other or react disproportionally."[62] In her opinion, anticipatory self-defence challenges the principles of necessity and, most importantly, of proportionality.

Nevertheless, many States and scholars have argued in favor of an anticipatory right of self-defence. Expecting from a State to be willing to wait to suffer an attack before defending itself, when there is evidence that it will be the target of an imminent armed attack, is thought to be unrealistic. The principle of necessity would not be challenged, since the resort to force in self-defence, be it after the armed attack has occurred or be it in anticipation of an imminent armed attack, is lawful only when other non-forceful means - such as diplomacy or law enforcement - fail to resolve the situation. For what concerns proportionality, the use of force in anticipatory self-defence can still be proportionate to the aim of halting the imminent armed attack, even if it has not occurred yet.

Nowadays, anticipatory self-defence, intended as the resort to force in anticipation of an *imminent* armed attack, has achieved broad acceptance amongst the international community. Geoffrey S. DeWeese states that it has become part of customary international law, as there are a good number of examples that prove that States have been resorting to force in anticipation of an armed attack.[63]

Defining what pre-emptive self-defence is has proven to be confusing. A number of scholars, as Gill and Ducheine, consider pre-emptive self-defence as a synonymous of anticipatory self-defence, that they define as: "defensive measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future."[64] Other scholars, as Michael Reisman, differentiate the two terms and attribute them slightly different meanings, for anticipatory self-defence being a response to a "palpable and imminent threat,"[65] while pre-emptive self-defence being a subset of this wider concept. The 'Bush Doctrine', that will be explained in the paragraphs below, offers an example of pre-emptive self-defence in the

---

[62] Christine Gray, "The use of force and the international legal order", p. 614.

[63] Geoffrey S. DeWeese, "Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence", in *2015 7th Conference on Cyber Conflict: Architectures in Cyberspace*, eds. M.Maybaum, A.M.Osula (Tallinn: 2015 NATO CCD COE Publications, 2015), p. 83.

[64] Terry D. Gill and Paul A.L. Ducheine, Anticipatory Self-Defense in the Cyber Context, p. 89, in Geoffrey S. DeWeese, "Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence", in *2015 7th Conference on Cyber Conflict: Architectures in Cyberspace*, eds. M.Maybaum, A.M.Osula (Tallinn: 2015 NATO CCD COE Publications, 2015), p. 85.

[65] Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Preemptive Self-Defense*, 100 A.J.I.L (2006), p. 526 in Geoffrey S. DeWeese, "Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence", in *2015 7th Conference on Cyber Conflict: Architectures in Cyberspace*, eds. M.Maybaum, A.M.Osula (Tallinn: 2015 NATO CCD COE Publications, 2015), p. 85.

meaning of Reisman. If the two concepts were to be regarded as separate, what would differentiate them would be mostly the level of imminence required for the anticipatory or the pre-emptive right of self-defence to be triggered. In fact, while for anticipatory self-defence the armed attack is palpable, for pre-emptive self-defence the realization of the armed attack is slightly more distant in time, but it is still considered to be an imminent threat to the national security of a State.

The disagreement over the lawfulness of anticipatory self-defence and of pre-emptive was so strong that no provision of it was included in the *Definition of Aggression* or in the *Declaration on Friendly Relations* of the United Nations General Assembly. Even the ICJ decided not to take a stand on the matter and left the controversy unresolved both in the *Nicaragua* case and in the *Armed Activities on the Territory of the Congo* case.

The notion of pre-emptive self-defence can be said to have evolved in two ways: the 'global war on terror' launched by the United States through *Operation Enduring Freedom*, and the fight against the proliferation of nuclear weapons, undertaken by the United States against the production of Weapons of Mass Destruction (WMD) by Iran, Iraq and North Korea.

2.2.3 Pre-emptive self-defense and the 'global war on terror'

After the 9/11 attacks against the Pentagon and the World Trade Center, the United States launched *Operation Enduring Freedom* in order to disrupt the use of Afghanistan as a territorial base for Al-Qaeda. Even though the terrorist attacks had not been conducted by Afghanistan itself, the United States justified its operation conducted in the territory of Afghanistan as self-defence. *Operation Enduring Freedom* was broadly supported by the International Community, that almost universally accepted the operation as self-defence. The UN Security Council explicitly recognized the right of self-defence in Resolution 1368, condemning the terrorist attacks. In its Resolution 1373, the UNSC envisaged individual and collective self-defence as possible measures against international terrorism, recognizing for the first time the right of self-defence against terrorist actions. This new scenario challenged the traditional scope of the right of self-defence.

On the one hand, the fact that *Operation Enduring Freedom* was justified as self-defence against the terrorist organization Al-Qaeda widened the notion of armed attack -originally intended as attack by a State - and the scope of self-defence, by allowing uses of force in self-defence other than against a sovereign State.

On the other hand, the fact that the International Community was supporting *Operation Enduring Freedom* seemed to demonstrate its approval for pre-emptive self-defence, at least in this particular case, and the establishment of instant customary international law. As Gray explains, the main goal the United States wanted to achieve with the launching of its military action was to deter *future* attacks against the US, while the main goal of the UK, who participated in the operation, was to avoid the enduring threat of attacks from Al-Qaeda. Both the US and the UK wanted to avoid future attacks, but were claiming to be acting in self-defence, although the initial attack had ended. Furthermore, the United States clearly stated that *Operation Enduring Freedom* had to be seen as a 'global war on terror' that could last many years. Therefore, what emerges from this extensive interpretation of self-defence supported by the United States is that the right of self-defence becomes a right of pre-emptive self-defence, now encompassing also operations addressing non-state actors.

It can be noted that this extensive interpretation of the right of self-defence carries many risks with it. If the goal of pre-emptive self-defence is to prevent future attacks, when can an armed attack be thought to be imminent enough in order to justify a pre-emptive self-defence action?

From the United States' standpoint, the "absence of specific evidence of where an attack will take place or of the precise nature of an attack does not preclude the conclusion that an armed attack is imminent."[66] Following their reasoning, the trigger of the right of pre-emptive self-defence shifts from imminence in time to the *likely* scale of the attack, and to the *likely* consequences it could provoke, as well as on the possibilities, if existing, to respond to an attack in self-defence.

If this interpretation of the right of pre-emptive self-defence were to be universally adopted, States would enjoy an extremely wide discretion in the application of the right to resort to force in self-defence.

---

[66] Christine Gray, "The use of force and the international legal order", p. 616.

2.2.4 Pre-emptive self-defence revisited? Halting the proliferation of nuclear weapons

Following the beginning of *Operation Enduring Freedom* in Afghanistan, the United States started focusing on the threats posed by the development of Weapons of Mass Destruction, especially in Iraq, Iran and North Korea. The United States, determined to halt the threat of the use of weapons of mass destruction at the hands of the so-called rogue States and global terrorists, urged a revision of the law of self-defence so that it would fit the needs of the nuclear era. Both in its *National Security Strategy* of 2002 and of 2006, the United States argued that it was necessary to reconsider the requirement of imminent attack for the applicability of the pre-emptive right of self-defence, adapting it to the capabilities and objectives of the contemporary adversaries. However, how the requirement of imminent attack had to be changed so as to trigger pre-emptive self-defence actions was not made clear or further elaborated on. This new and more extensive perception of pre-emptive self-defence has been best classified as 'preventive self-defence'. Preventive self-defence is, in fact, the resort to force employed to counter threats that are not imminent; it is a response to a undefined or even potential threat of attack that could occur at some indeterminate point in the future, even in a matter of years.

Already in 2004, the High-level Panel of Experts established by the United Nations had strongly rejected this doctrine. In its report, the High-level Panel of Experts had affirmed that there was no right to self-defence if the threat of armed attack was not imminent. In case there was clear evidence of an imminent threat of armed attack and solid arguments to support the necessity of (pre-emptive) military actions, it was in the hands of the United Nations Security Council to authorize the military actions that it deemed necessary to halt the threat.[67] The view of the UN High-level Panel of experts was reinforced by the International Court of Justice in 2005, that affirmed likewise that the meaning of Article 51 should be left to what the provision actually states, and that the UN Charter had set out other measures that did not include the use of force to solve international issues or protect security interests, including the recourse to the Security Council.

In any case, this controversial doctrine was regarded with considerable suspicion by the majority of States. Although *Operation Enduring Freedom* had been widely accepted and

[67] ibid., p. 617.

supported, the international community did not seem to be willing to accept a further extension of the right to anticipatory self-defence, that is to say, States were not willing to "abandon the requirement that for self-defence to be permissible a terrorist attack should already have occurred, be underway, or at the most extensive, imminent."[68]

2.2.5 Collective self-defence

The inclusion of the right of collective self-defence into Article 51 of the UN Charter is seen as an innovation compared to the pre-existing right of self-defence. It was used as a basis for the building of military alliances, such as the North Atlantic Treaty Organization (NATO)[69] and for the drafting of collective self-defence treaties, such as the Warsaw Pact.[70] However, there is disagreement as to whether collective self-defence represents a valuable safeguard for smaller States or if, on the contrary, it endangers them by providing powerful States a lawful justification for their intervention in conflicts of other States.[71]

When the right of collective self-defence was used as a justification for the intervention of a State in the conflict of another State, controversies arose with regard to the assessment of the action that had supposedly triggered the right of self-defence, that is to say, with regard to the classification of the offensive action as armed attack, as well as to whether there had been a request by the victim State for collective self-defence.

The *Nicaragua* case set out the parameters for the lawful exercise of the right of collective self-defence. In the aforementioned judgement, the International Court of Justice condemned the unlawful intervention in alleged collective self-defence of the United States by explaining that 1) there had been no armed attack by Nicaragua triggering the right of self-defence for Honduras, El Salvador, or Costa Rica; 2) in the eventuality that an armed attack

---

[68] Christine Gray, *International Law and the Use of Force*, p. 177.

[69] The North Atlantic Treaty, also referred to as Washington Treaty, established the North Atlantic Treaty Organization (NATO) in 1949. Collective self-defence is envisaged by its Article 5, for which an attack against an Ally is considered as an attack against all Members of the military alliance.

[70] The *Warsaw Treaty of Friendship, Cooperation, and Mutual Assistance*, also referred to as Warsaw Pact, was a treaty establishing the Warsaw Treaty Organization, a military alliance between the Soviet Union, Albania, Bulgaria, Czechoslovakia, East Germany, Hungary, Poland and Romania. The organization was in place between 1955 and 1991. The treaty established a unified military command and allowed the stationing of Soviet troops on the territories of the other Member States.

[71] Christine Gray, "The use of force and the international legal order", p. 618.

had taken place, there had been no declaration of such States that they were victims of an armed attack; 3) the supposed victim States had not made an invitation to the US for aid; 4) the United States had not reported its actions to the Security Council under Article 51.

As it can be understood from the judgment, the criteria set out by the ICJ for the lawful exercise of collective self-defence are: 1) the occurrence of a use of force that reaches the threshold of an armed attack as *conditio sine qua non* for the exercise of the right of (individual and) collective self-defence; 2) the declaration of the victim state that it suffered an armed attack; 3) the request for assistance by the victim State to a foreign State, invoking the right of collective self-defence, after which the foreign State can intervene and help the victim State to repel the attack; 4) the duty to report the intent of acting in collective self-defence under Article 51 to the Security Council.

The judgment of the ICJ was criticized for applying a narrow interpretation of the meaning of armed attack and for imposing restrictive requirements to the right of collective self-defence, namely that of a declaration of the victim state to have been the target of an armed attack, and that of its request for assistance. The scholars who criticize the judgment of the Court believe that such requirements would prevent the weak victim State from being protected from oppression. However, as a matter of fact, the Court's position reflects State practice on collective self-defence. State practice shows that usually a declaration by the victim State about the fact that it suffered an armed attack and a request for assistance to foreign States would be made. The Rio Treaty,[72] for example, explicitly requires a request by the victim State in order for the other Member states to intervene in collective self-defence. Furthermore, those in support of the Court's decision argue that a wider interpretation of the right of collective self-defence could translate into a threat to international peace. In their opinion, a lower threshold of armed attack and the absence of a distinction between the 'most grave forms' and the 'less grave forms' of the use of force, and thus a wider applicability of the right of self-defence - individual or collective-, could lead to an increase in the involvement of powerful States. Consequently, this would lead to an increase of the risk of the "internationalization of civil conflicts and the expansion of inter-state conflicts."[73]

---

[72] The *Inter-American Treaty of Reciprocal Assistance*, commonly referred to as Rio Treaty, was signed in 1947 in Rio de Janeiro among the countries of the Americas. As the Washington Treaty, it established that an attack against one of the Member States is an attack against of Member States. Furthermore, in its Article 3(2), it sets as requirement for the collective self-defence action the request of the victim state or states directly attacked.

[73] Christine Gray, *International Law and the Use of Force*, p. 156.

3. The notion of 'armed attack' and International Humanitarian Law

International Humanitarian Law, or the Law of Armed Conflict, is the body of law that regulates the conduct of hostilities in order to "minimize harm during an armed conflict that is either unnecessary to effectively accomplish legitimate military aims or excessive relative to them. It does so by establishing legal boundaries for the conduct of 'attacks'."[74]

The most significant steps of the establishment of International Humanitarian Law have been the entry into force of the Hague Conventions of 1899 and 1907, and the four Geneva Conventions of 1949 together with their two Additional Protocols of 1977. The Law of the Hague deals with the regulation of belligerency among the belligerents and the relations among the belligerents and neutral states, while the Law of Geneva deals with the protection of wounded and sick soldiers on land during war (GC I); the protection of wounded, sick and shipwrecked military personnel at sea during war (GC II); prisoners of war (GC III); and lastly with the protection of civilians, including in occupied territories (GC IV).

Thanks to the Geneva Conventions of 1949, that represent the cornerstone of the Law of Armed Conflict, the laws of war are applicable not only in the event of a 'war', but also in the event of an 'armed conflict', both international and non-international in nature. The identification of a 'state of war', through a formal declaration of war or another formal pronouncement, is not a *conditio sine qua non* for the applicability of the Laws of War anymore. Although the classification of conflicts is still very relevant for the applicability of the law, the classification of a conflict as *war* is not determinant anymore from a legal standpoint when it comes to the applicability of most of the principles of International Humanitarian Law.[75] Article 2 common to the four Geneva Conventions of 1949 states that the conventions shall apply to "[...]all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.[...]"

Furthermore, the Preamble to Additional Protocol I of 1977 to the Geneva Conventions on the Protection of Victims of International Armed Conflicts provides that:

---

[74] Michael N. Schmitt, ""Attack" as a Term of Art in International Law: The Cyber Operations Context", p. 285.

[75] Such statement can be challenged by considering what stated above from the perspective of the Law of Neutrality, but considerations in this regard fall outside the scope of the present work, and thus implications about the Law of Neutrality will not be made.

> "[...] the Provisions of the Geneva Conventions of 12 August 1949 and of this Protocol must be fully applied in all circumstances to all persons who are protected by those instruments, without any adverse distinction based on the nature or origin of the armed conflict or on the causes espoused by or attributed to the parties to the conflict."[76]

The extension of the applicability of the Laws of War from a declared 'state of war' - as established by Article 1 of the Hague Convention No. III of 1907 relative to the Opening of Hostilities - to a 'state of armed conflict' - as expressed by the Art. 2 common to the Geneva Conventions - comes from different reasons. Firstly, the entry into force of the UN Charter of 1945 has made "the declaration of war redundant as a formal international legal instrument."[77] A 'state of war' is believed to be incompatible with the UN Charter regime by many scholars. The compatibility of a 'state of war' with the UN Charter regime has also been argued in a set of debates at the UN Security Council.[78] Secondly, State practice shows that "there have been no formal declarations of war since the Soviet declaration of war on Japan in August 1945."[79] Finally, the development of new means and methods of warfare, and thus the changing nature of warfare itself, has required for the Laws of War to have a wider scope.

As Greenwood explains, 'war' has lost its *legal* significance, but it has gained a *factual* significance. Nowadays, the explicit identification of a conflict as 'war' implies the intention of the attacking State to severely defeat the enemy, that its war aims are extensive and/or that the conflict is on a large scale.[80]

---

[76] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 8 June 1977*. Preamble.

[77] David Turns, "The Law of Armed Conflict (International Humanitarian Law)", in *International Law*, ed. Malcolm D. Evans (New York, Oxford University Press, 2018) (fifth edition), p. 844.

[78] The debate over the incompatibility of the UN Charter regime and the creation of a 'state of war' was advanced by Israel during a debate at the United Nations Security Council in 1951. The issue being discussed was the legality of Egypt's action against the shipping passing through the Suez Canal bound to or from Israel. The state of war between the two States had been ended with the signing of the armistice in 1949, but Egypt was still claiming its lawful exercise of belligerent rights. The representative of Israel asserted that, due to the establishment of the UN Charter regime now regulating International Relations, Egypt could not exercise its belligerent rights. Under the UN Charter regime, in fact, States were pledged to refrain from the threat or the use of force in their international relations, except for the purposes admitted by United Nations itself - namely, self-defence. The representative of Israel further explained that there could be no doctrine of belligerency since belligerency was seen as a political or legal mean regulating the threat or use of force. Israel's position regarding the issue was not endorsed in the UNSC Resolution, but it opened the ground for further discussion among a number of writers. See: Christopher Greenwood, "The Concept of War in Modern International Law.", p. 287-290.

[79] David Turns, "The Law of Armed Conflict (International Humanitarian Law)", p. 844.

[80] Christopher Greenwood, "The Concept of War in Modern International Law.", p. 297.

However extensive the war aims of a State may be, it is believed to be more convenient for States to refrain from an explicit declaration of war and thus of hostile intent, since a *status mixtus* allows more room of maneuver to achieve both political and diplomatic goals. The classification of a conflict as **'**war' would frustrate diplomatic and economic relations, as well as the operation of treaties to which the states at war are parties, while the fighting in absence of a formal declaration of war allows for the application of the laws of peace and of the laws of war simultaneously.

To sum up, the application of International Humanitarian Law in no way depends on the formal recognition of the fighting as 'war' or as 'armed conflict', nor on the alleged legality or illegality of the initial resort to force. Nevertheless, the question of when and how humanitarian law applies is not so straightforward, partially because the term 'armed conflict' has not been defined, and partially because of the evolution of the means and methods of warfare and of armed conflicts themselves.

3.1 The classification of 'armed conflicts' and the scope of International Humanitarian Law

The difficulty in determining the precise scope of International Humanitarian Law lies in the lack of a formal definition of 'armed conflict' for the purposes of application of the law, notwithstanding the use of the term in the Geneva Conventions and in other treaties that compose IHL itself.

The International Criminal Tribunal for the Former Yugoslavia (ICTY) defined the term 'armed conflict' in the *Tadić* case in 1995, by stating that "an armed conflict exists whether 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."[81]

Michael N. Schmitt classifies the types of armed conflicts that fall under the scope of International Humanitarian Law as follows. He argues that 'armed conflict' is a legal term of art that refers to two types of conflicts, namely international armed conflicts and non-

[81] *Prosecutor v Duško Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Interlocutory Appeal), Case No IT-94-1-AR72 (2 October 1995) 35 ILM 35, para 70.

international armed conflicts. In the former case, the conflict takes place between two or more States; in the latter one, the conflict takes place between a State and an internal organized armed group or among organized armed groups of the same State. Non-international armed conflicts may be further divided into 1) non-international armed conflicts inside the territory of a State; 2) non-international armed conflicts that have transnational effects or 'spillovers'. Additionally, a non-international armed conflict may become international in character due to the change in the legal personality of one of the parties or to the involvement of foreign forces.[82] It is important to take into account, however, that not all the provisions of IHL apply in case of non-international armed conflict, such as the qualification of combatant and of prisoner of war status.

Art. 1(4) of AP I extends the applicability of the Law of Geneva to "[...] armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist régimes in the exercise of their right of self-determination."[83]

In the event that the situation in question lacks of the characteristics explained above, it would not fall under the scope of IHL, and it would be governed by domestic and human rights law instead.[84] Furthermore, the ICTY set a timeframe for the application of IHL in the *Tadić* case, stating that:

> "[...] International Humanitarian Law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring State or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there."[85]

All that was explained above is now recognized as customary international law, as well as the implicit requirements for hostilities to be substantial, protracted, and large-scale, as expressed by the ICTY in *Tadić*.[86] This implies that minor or limited military operations conducted in absence of a pre-existing armed conflict, and that are not substantial, protracted and large-scale would not fall under the scope of International Humanitarian Law. The same reasoning can be applied to minor armed incidents across international borders, for instance. Despite the

---

[82] David Turns, "The Law of Armed Conflict (International Humanitarian Law)", p. 846-847.

[83] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 8 June 1977. *Article 1(4)*.

[84] Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, p.285

[85] *Prosecutor v Duško Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Interlocutory Appeal), Case NO IT-94-1-AR72 (2 October 1995) 35 ILM 35, para 70.

[86] David Turns, "The Law of Armed Conflict (International Humanitarian Law)", p. 845.

possibility of deploying military forces without being subject to the application of the Law of Armed Conflict, it has been observed in state practice that the governments of the major military powers require their armed forces to comply with the principles of LOAC even when undertaking minor military operations. Thus, the continual exercise of armed violence in an armed conflict is not necessary for the Law of Armed Conflict to be applicable. In fact, as expressed in *Tadić* by the ICTY, some of the provisions of the Law of Armed Conflict persist even after the cessation of hostilities.

Finally, it is important to note that the same rules apply to four of the four domains of warfare: land, sea, air, outer space. The rules applicable to every domain have been formulated on the basis of the rules governing land warfare, and have been restated taking into account the peculiarities of each domain. Rules on maritime warfare[87] and on aerial warfare[88] have been broadly accepted by the international community. With concern to the fifth domain of warfare, namely cyberspace, consensus has not been reached with regard to the potential rules regulating cyber warfare. Even though the international community lacks of a binding document regulating cyber warfare, most of the principles of International Humanitarian Law are applicable to cyber warfare thanks to the Martens Clause, included in the Preamble of the Hague Convention (IV) of 1907, in the four Geneva Conventions of 1949 and in Additional Protocol I of 1977. The clause states 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 usage established between civilized nations, from the laws of humanity and the requirements of the public conscience."

How International Humanitarian Law should be applied to cyber warfare will be a matter of discussion in Chapter 3.

---

[87] See: *San Remo Manual on International Law applicable to Armed Conflicts at Sea*, 12 June 1994.

[88] See: Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge: Cambridge University Press, 2013).

3.2 The Conduct of Hostilities

As explained above, International Humanitarian Law establishes rules regulating both the protection of civilians during international and non-international armed conflicts, and the means and methods of warfare. For the purpose of my thesis, this work will be focused on the latter.

The conduct of hostilities, generally referred to as means and methods of warfare, is regulated by the 1907 Hague Regulations, together with certain provisions of Additional Protocol I to the four Geneva Conventions of 1949. Such conventions form the so-called 'law of targeting', which fundamental principles are the rules of distinction and proportionality, and the prohibition of the use of certain weapons that can cause unnecessary suffering or superfluous injury. Furthermore, the law on the conduct of hostilities also distinguishes between battlefield practices that are allowed under its rules and the ones that are forbidden. Sabotage or espionage are not forbidden under LOAC for instance, while acts of perfidy are.[89]

3.2.1 Distinction and Proportionality

Given the importance of the respect for and protection of civilians in International Humanitarian Law, the principle of distinction is one of its core rules. It forms part of Customary International Law and it is codified in Article 48 of AP I, that states:

> "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."

Belligerents are obliged at all times to distinguish between military objectives and civilian objects, and are allowed to attack only the former. In fact, Article 51(2) of AP I clearly

[89] Perfidy is defined by Article 37 (1) of Additional Protocol I of 1977 to the four Geneva Conventions of 1949 as "[...] Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy." The same Article provides examples of perfidy, that are "(a) the feigning of an intent to negotiate under a flag of truce or of a surrender; (b) the feigning of an incapacitation by wounds or sickness; (c) the feigning of civilian, non-combatant status; and (d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict."

prohibits attacks on the civilian population, as well as those attacks whose purpose is spreading terror among the civilian population.

What constitutes a military objective is explained in Article 52(2) of the same Protocol, that states that:

> "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 or neutralization, in the circumstances ruling at the time, offers a definite military advantage."

As for the nature of an object, an object is inherently military in nature when it is designed and created for military aims only, such as military bases, ports or airfields, military vehicles, weapons, and ammunitions. As for the location of a military object, we intend the location of an object that has military significance, such as a crossroad or rail yards. As for the purpose of an object, a military object is one that is *intended* to be used for military action, such as industrial installations producing material for armed forces. Other objects that may constitute military objectives are, among others, transportation systems for military supplies, conventional power plants, and fuel dumps.

Those objects that are not intrinsically military in nature, but that make an effective contribution to the military action of the adversary, could be the target of an attack as well. This is the case of those objects which were designated for purposes other than the military one - such as a school, or a civilian house - which have been converted to military use in times of hostilities. Such concept is expressed by Rule 10 of the ICRC Customary International Law Study, that states that civilian objects are protected against attack, unless and for the time as, they become military objectives. So, when a civilian object is used in such a way that it loses its civilian character and qualifies as a military objective, it is liable to attack.

However, in modern warfare, the distinction between civilian objects and military objectives is not always straightforward. For this reason, "in case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be used."[90]

---

[90] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, Art. 52(3).

Although the principle of distinction aims at avoiding the injury or loss of civilian lives, as well as the damage or destruction of civilian objects, it is often impossible to avoid 'collateral damage', even when undertaking a lawful military attack. For such reason, the principle of distinction is moderated by the principle of proportionality, or the so-called 'proportionality test'. Before launching an attack, the commander is obliged to calculate if the incidental loss of civilian life, injury to civilians, damage or destruction to civilian objects expected to be caused as 'collateral damage' of a lawful attack on a military target are proportional to - or not excessive in relation to - "the concrete and direct military advantage anticipated from the attack."[91] Therefore, International Humanitarian Law "accepts that at least some civilian casualties and/or some damage to civilian objects will be inevitable in most military operations, however carefully conducted."[92]

It is evident that the provisions of the Protocol favor the protection of civilians over the achievement of military goals. In doing so, they place a great amount of responsibility in the hands of the attacking commander who, apart from having to take all the precautions necessary in the planning and in the launching of the attack, has to alert the civilian population, make sure to limit civilian casualties and even suspend a military attack if it becomes evident that the collateral damage would be disproportionate to the actual military advantage.[93] According to the rule of precaution, the commander has to verify that the objectives to be attacked are in fact legitimate military objectives, she/he has to choose means and methods of warfare to avoid or minimize collateral damage, and she/he has to refrain from the launching of an attack which does not meet the proportionality test.

3.2.2 Weaponry

The 1907 Hague Conventions restrict the right of belligerents to adopt means to injure the opponent, affecting the choice of weaponry in armed conflicts and the methods of its employment. The restrictions on the choice of weaponry and on its use, together with the aforementioned principle of distinction, give rise to two customary rules: 1) It is prohibited to

[91] David Turns, "The Law of Armed Conflict (International Humanitarian Law)", p. 857.

[92] ibid.

[93] ibid., p. 858.

employ means and methods of warfare that may cause unnecessary suffering or superfluous injury; 2) it is prohibited to employ means and methods of warfare that are indiscriminate.[94]

With regard to the former prohibition, the principle is envisaged both in Article 23 (e) of the 1907 Hague Convention (IV) and in Article 35 of AP I. While in the 1907 Hague Convention (VI) the phrasing 'calculated to cause unnecessary suffering' refers to the use of military items with the *intention* of causing unnecessary suffering, in Article 35 (2) of AP I the prohibition is directed to the employment of weapons that are 'of a nature to cause' unnecessary suffering. From such prohibition derive many treaties banning the use of specific weapons. It is important to point out that the suffering caused by an attack has to be balanced with the principle of humanity. In this context, in fact, the attack with a certain weapon is lawful when it causes the suffering necessary to achieve certain military aims, as disabling the armed forces of the enemy, for instance. An attack carried out with a lawful weapon would, in fact, injure to disable and not injure to kill. What is the threshold of the permissible level of disablement, however, is not specified, nor is the concept of unnecessary suffering further defined.

With regard to the ban of indiscriminate weapons, the provision is expressed by Article 51 (4) and (5) of Additional Protocol I. It forbids indiscriminate practices such as the bombing of large areas that include civilian objects or the presence of civilians, for instance.

In addition to these rules of customary law, many treaties have been made over the years so to ban or restrict the use of certain weapons, such as bacteriological and chemical weapons or incendiary weapons. For what concerns nuclear weapons, there is not an explicit prohibition of their employment in International Humanitarian Law yet, although their use has been condemned both by the United Nations and by the ICJ in its *Advisory Opinion on Nuclear Weapons*.[95]

---

[94] ibid., p. 859.

[95] *Legality of The Threat or Use of Nuclear Weapons*, *Advisory Opinion*, I.C.J. Reports 1996, p. 226.

3.3 The meaning of 'attack' under International Humanitarian Law

The meaning of attack under IHL is different than the one under the *jus ad bellum*. In fact, in International Humanitarian Law, the term 'attack' triggers a wide range of legal protections and restrictions, as explained above. Many of LOAC's fundamental rules on the conduct of hostilities, as we have seen, are expressed in terms of attacks. Listing some examples, in the case of rules protecting civilians, such as Article 51(2) of AP I, that states: "the civilian population as such, as well as individual civilians, shall not be the object of attack", and Article 51(4) of AP I that states: "indiscriminate attacks are forbidden", it is evident that one of the most important purposes of International Humanitarian Law is that of minimizing the severity of *attacks* and their consequences. For what concerns the principle of precaution, its rules - as Arts. 57 and 58 of AP I - address both attacks themselves and their effects.[96] The main purpose of IHL itself is that of restricting the lawfulness of attacks, and thus the possibility of States to severely harm their opponents during armed conflicts.

In International Humanitarian Law, the term refers to a particular category of military operations. Article 49(1) of AP I provides the definition of the term 'attack', stating that attack means "acts of violence against the adversary, whether in offence or defence." It is considered a neutral term in the sense that it does not equate to 'illegal', since not all attacks are unlawful, given that they respect the prohibitions and restrictions of the law. Even though it is a neutral term, "attack is operatively a key threshold concept in [IHL] because many of its core prohibitions and restrictions apply only to acts qualifying as such."[97]

The definition given by Art. 49(1) of AP I has triggered significant debate as to whether acts of violence are recognized to be only kinetic in nature or if they can be also non-kinetic. In the words of Nils Melzer,

> "[t]oday, it seems to be generally recognized that 'acts of violence' do not necessarily require the use of kinetic violence, but that it is sufficient if the resulting effects are equivalent to those normally associated with kinetic violence, namely death or injury of persons or the physical destruction of objects [...]."[98]

---

[96] Nils Melzer, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research, 2011, p. 25.

[97] Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, p. 285.

[98] Nils Melzer, *Cyberwarfare and International Law*, p. 26.

Concerning cyber operations, it has been recognized that they constitute attacks regulated by LOAC when they are capable of triggering processes likely to cause injury, death or destruction. The matter will be explained in details in Chapter 3.

4. Cyber warfare and cyber operations: new challenges for International Law

The advances of information and communication technology (ICT) have brought numerous advantages together with many threats to national and international security. Those developed States that were considered to be the safest from the perspective of national security and capable of self-defence - because of their strong military capabilities -, are thought to be not so secure from the point of view of cybersecurity because of their high dependency from ICT. Such States, in fact, are the most suitable targets of malicious cyber operations and/or of cyber attacks due to the fact that they extensively rely on computer systems and networks for the functioning of the state apparatus and civil society. Cybersecurity-related strategies and concerns have been included in the National Security Strategies of several States in the past two decades. However, due to the fact that the boundaries of what is what in the cyber realm have not yet been traced, the international community is struggling in finding agreement over the definitions of 'cyber warfare' and of 'cyber operations' and their regulation under International Law. Moreover, the lack of shared definitions makes it difficult for policy makers of different countries to develop collective and coordinated policy recommendations, and for governments to take concerted actions. Attempts have been made both nationally - among the different sections of the state's military apparatus - and internationally to define the terms of the cyber domain, with poor results. The difficulties that the international community is encountering are many: from the problem of attribution of a cyber activity to a State, to the inner abstractness of the cyber real, the new domain surely poses new challenges to international law.

Due to the blurry terminology, the first effort that will be made in this dissertation is that of displaying the most adopted and accepted definitions of 'cyber warfare' and of 'cyber operations', as well as the classification of such operations and the effects they can manifest.

This is believed to be the first fundamental step towards the legal regulation of the always-increasing threat posed by malicious cyber-operations.

4.1 Terminology: definitions and classification

The most significant government-led efforts to define cyber warfare and cyber attacks have been made on the one side by the United States, and on the other side by Russia and China. While the United States National Research Council (NRC) focused on defining the terms 'cyber attack' and 'cyber warfare', the Shanghai Cooperation Organization (SCO)[99] - led by Russia and China - focused on defining the term 'information war'. In the first case, the United States NRC defined cyber attacks as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks,"[100] restricting their notion to those hostile actions that intend to harm a cyber system. This vision was confirmed by the United States Cyber Command (USCYBERCOM) that, together with the US Joint Chiefs of Staff, defined cyber-attacks from a military standpoint as "hostile act[s] using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[101]

The Shanghai Cooperation Organization took a different path and did not define cyber attack or information attack and/or information operation, but limited itself to defining 'information war' as:

> "a confrontation between two or more states in the information space with the aim of damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems, psychologically manipulating masses of the population to destabilize society and the State, and also forcing the state to take decisions in the interest of the opposing party."[102]

---

[99] The Shanghai Cooperation Organization is a Security Cooperation Group founded in 2001 whose members are China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russian Federation, Tajikistan and Uzbekistan. The group counts also of four observers, namely Afghanistan, Belarus, Iran and Mongolia.

[100] William A. Owens et al., National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities*, The National Academy of Sciences, 2009, p. 1.

[101] Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations, November 2011, p. 5.

[102] Shanghai Cooperation Organization, *Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*, 61st Plenary Meeting (2 December 2008), Annex 1.

As can be noted in the definition of information war, the SCO includes not only the actions that aim at damaging information systems, but also those actions that aim at manipulating masses of the population and at destabilizing society, attributing them also the capability of influencing the political stability of a country. The perspective of the Shanghai Cooperation Organization greatly differs from the one of the United States. The U.S. Government, in fact, understands cyber attacks as intended to disrupt or destroy computer systems or networks only. As a matter of fact, the psychological element present in the SCO's definition is not present in the United States' one. The differing views come from a distinct perception of the possible threats to national and regional security and to political stability, as well as from different political doctrines.

This example has made self-evident the fact that giving a common definition to cyber-attacks is not easy because it involves not only diverse legal opinions and traditions, but also different political, factual, strategic, and doctrinal views. However, defining the terms of cyber domain is crucial for the creation and/or adaptation of proper laws and for giving appropriate legal responses to current issues in such domain.

In the last two decades, the lexicon used by writers has changed together with the evolution of the field. Nowadays, whereas Russian experts still push for official and internationally agreed definitions, most scholars and experts in the field have adopted the United States Department of Defense (DoD) Terms and Definitions glossary.

Initially, many legal analysts talked about 'information warfare' based on the analysis provided by Martin Libicki in his "*What is Information Warfare?"* of 1995. In his seminal work, Libicki defined information warfare compatibly with the current definition of 'information operations', an 'umbrella term' that comprises different subcategories. In fact, in military doctrine, 'information operations' are a macro-category of operations defined as:

> "[the] integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[103]

This macro-category included 'Computer Network Operations' (CNO), term introduced by the United States DoD in 2006 and extensively used by scholars up until 2010. Computer

[103] US Department of Defense, *National Military Strategy for Cyberspace Operations*, 2006, p. GL–2.

Network Operations consist of computer network attacks (CNA), computer network defense (CND), and computer network exploitation enabling operations (CNE).

CNAs are defined by the US *National Military Strategy for Cyberspace Operations* (NMS-CO) as "operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves." The *NATO Glossary of Terms and Definitions* adopts the same view on the matter. Both the NMS-CO's and NATO's definitions distinguish between those CNAs whose target is the *information* contained in the computer or computer network, and those computer network attacks whose target is the computer or the computer network itself.[104] The definitions given focus on the targets of a CNA, but do not indicate what are the *means* through which such attacks can be carried out; in fact, the launching of a computer network attack through kinetic or electronic means is not excluded, for instance.

In 2010, the *Joint Terminology for Cyberspace Operations* replaced the US DoD's existing definition of CNA by introducing a more complete description. According to such, a CNA is:

> "[a] category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves. [...]."

In this case, the definition takes into account the means through which a CNA can be launched and makes explicit that the attacks that are considered as computer network attacks are those conducted through the use of computer networks only.

To sum up, the defining feature of CNAs is that both the target of the attack and the means employed to carry it out are to be found in the network itself or in the information it contains. This feature of CNAs distinguishes them from electronic operations and electronic warfare, for instance. In the latter case, although the aim could be that of destroying a network as well, attacks are delivered by using electromagnetic energy - such as electromagnetic pulse generators. A CNA, instead, delivers an attack by using computer code.

Computer Network Defense (CND) is defined by the US *National Military Strategy for Cyberspace Operations* as those actions "[...] taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks."

---

[104] The *NATO Glossary of Terms and Definitions*, in its Edition 2019, defines CNAs as: "action[s] taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself." in North Atlantic Treaty Organization. *NATO Glossary of Terms and Definitions in English and French. Glossaire OTAN de termes militaires et definitions en englais et française,* p. 30.

CNDs can be both active and passive. Active CNDs are attacks in response to a previous cyber attack. Passive CNDs, instead, are actions taken to defend the networks of a State and can consist in the use of prevention devices and/or intrusion detection devices, for instance.[105]
As noted by Roscini, the term 'computer network defence' was dropped in 2010 and replaced with the expression 'cyberspace defense', adopted by the United States *Air Force's Doctrine for Cyberspace Operations*. In this context, 'cyberspace defence' was defined as the "passive, active and dynamic employment of capabilities to respond to imminent or on-going actions against AF [Air Force] or AF-protected networks, AF's portion of the Global Information Grid or expeditionary communications assigned to AF."[106]
CNEs or 'computer network exploitation enabling operations' were defined in 2006 by the US *National Military Strategy for CyberSpace Operations* as "[e]nabling operations and intelligence collection to gather data from target or adversary automated information systems and networks;"[107] these operations must occur through the use of computer networks. Similarly, the *NATO Glossary of Terms and Definitions* defines CNEs as "[a]ctions taken to make use of a computer or computer network as well as the information hosted therein, in order to gain advantage."
However, in 2010 the term 'computer network operation' was substituted by the term 'cyber operation', because the former was considered to lead to the mistaken belief that computer networks were the only targets of such operations.

4.1.1 Cyber Operations and Cyber Attack

The United States DoD *Dictionary of Military and Associated Terms* defines cyber operations as the "employment of cyberspace capabilities where the primary purpose is to achieve primary objectives in or through cyberspace,"[108] suggesting that cyberspace can be both the target and the means through which an attack is delivered. However, the DoD does

---

[105] Marco Roscini, *Cyber Operations and the Use of Force in International Law,* (Oxford: Oxford University Press, 2014. Oxford Scholarship Online, 2014) p. 14. DOI: 10.1093/acprof:oso/9780199655014.001.0001.

[106] ibid.

[107] US Department of Defense, *National Military Strategy for Cyberspace Operations*, (2006), p GL–1.

[108] US Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, (8 November 2010 as Amended Through 15 February 2016) p. 121.

not go further in classifying the different types of cyber operations. The definition given by the DoD is confirmed by the definition of cyber operations given by the *Tallinn Manual on the International Law applicable to Cyber Warfare*, that affirms that a cyber operation is the "employment of cyber capabilities with the primary purpose of achieving objectives in or *by the use of cyberspace*."[109] Cyber operations can have different goals, such as infiltrating a system and collecting, exporting, destroying, or changing, encrypting data or triggering, altering or manipulating a set of processes controlled by the 'victim' computer system.[110] In contrast with CNOs, cyber operations can be carried out not only remotely - that is to say, through the use of networks-, but also though the physical installation of malware by a physical agent that has direct access to the system to be infected.

As for computer network operations, cyber operations is a macro-category inside which we can distinguish among 'cyber attacks', 'cyber defense' and 'cyber enabling operations', as explained by the US Joint of Chiefs Staff in the *Joint Terminology for Cyberspace Operations* of 2010.

What distinguishes a cyber attack from a CNA is that the latter is narrower than the former, in the sense that a cyber attack can be conducted not only through the network but also thanks to the possibility to physically deliver the attack by having access to the target system. Furthermore, a cyber attack differs from a CNA for its purpose: while a CNA only aims at damaging the network or the information it contains, a cyber attack can aim at degrading or destroying the critical infrastructure or the command and control (C2) capability of its target. In the words of the US Joint Chiefs of Staff, a cyber attack is:

> "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves - for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. [...]."[111]

The US Joint Chiefs of Staff designated that the term 'cyber attack' would replace 'CNA' and 'offensive cyberspace operations' when the hostile action reached the threshold of use of

---

[109] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* (Cambridge: Cambridge University Press, 2013), p. 258.

[110] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 11.

[111] Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Directors of the Joint Staff Directories, *Joint Terminology for Cyberspace Operations* (November 2011), p. 5.

force and/or when it specifically aimed at disrupting, denying, degrading, manipulating, and/or destroying the adversary computer systems or data, as they commented in the 2011 *Joint Terminology for Cyberspace Operations*.

According to the aforementioned Terminology, cyber defence is identified with the:

> "integrated application of DoD or US Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable US freedom of actions."

The Joint Chiefs of Staff also enlisted three different types of actions that constituted cyber defense. They explained that such definition replaces that of CND because the newly introduced term focused on mission assurance, introducing the concept of maneuver thanks to the allowance of proactive measures and military deception, for instance, while the older term was too narrow.

As for cyber enabling operations, their definition is not substantially different from the one given to CNEs.

Cyber attacks must be distinguished from cyber exploitation, that is the "unauthorized access to computers, computer systems, or networks, in order to exfiltrate information, but without affecting the functionality of the accessed system or amending/deleting the data resident therein."[112] The primary difference between cyber exploitation and cyber attacks lays in the nature of the payload they have to execute: the payload of cyber exploitation acquires information non-destructively, while the payload of a cyber attack is in itself destructive. Cyber exploitation can be preliminary to a kinetic attack or to a cyber attack, for instance, as it is used to for intelligence gathering,[113] for the surveillance of areas and/or people of interest, and for reconnaissance.[114]

For the seek of this dissertation - whose focus is that of cyber attacks and their regulation under International Law - and in agreement with the definition given by Roscini, for cyber attacks we intend those cyber operations whose aims are altering, deleting, corrupting, or denying access to computer data or software, with the purpose of :

---

[112] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 16.

[113] 'Intelligence gathering' is the process for which cyber exploitation collects information regarding enemy forces and activities, together with useful information to conduct one's operations'.

[114] 'Reconnaissance' consists in the observation or detection of information about the resources and activities of one's enemy.

> "[1)] propaganda or deception; and/or [2)] partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); [3)] producing physical damage extrinsic to the computer, computer system, or network."[115]

As will be explained in Chapter 2, cyber attacks may constitute 1) a 'threat or use of force' under Article 2(4) of the United Nations Charter; 2) 'armed attacks' as intended by Art. 51 of the same Charter, 3) or military operations during an armed conflict, and thus 'attacks' under International Humanitarian Law.

4.1.2 Cyber Warfare and Cyber War

As anticipated, the definition of information warfare given by the Shanghai Cooperation Organization did not receive international support apart from its member states. The discussion of the 2019 11th International Conference on Cyber Conflict brought to the drafting of two possible definitions on this regard: information warfare can be defined as the use of IT as active weapon of war - examples can be the interception, disruption, and defense of military-specific communications, IT, and critical computer systems; or as the strategic use of information to gain advantage with regard to the adversary.

Consequently, information operations are addressed to the adversary's information systems, and can be used to affect the adversary's information while defending one's own information system. The purpose of such operations would be the one of influencing, disrupting, or corrupting the adversary's human and automated decision-making.

For what concerns cyber warfare and cyber war, during the 2019 11th International Conference on Cyber Conflict scholars and experts did not reach any solid agreement with regard to their definition.

Traditional warfare is usually characterized by the violent struggle for domination between different States, alliances or coalitions, involving force-on-force military operations launched through different types of military capabilities against one another in the five domains of

[115] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 17.

warfare, namely land, air, sea, outer space and cyberspace. Behind military confrontations lie military and/or political objectives.[116]

One may wonder why not transposing the definition of traditional warfare to the cyber domain, adapting it to its peculiarities. However, the definition of cyber warfare is not so straightforward, and it can identify three different behaviors. Cyber warfare can be defined as:

1) the defense and/or the attack of information and computer networks, as well as the ability to deny the adversary of the possibility to do the same, or even as the domination of the information environment on the battlefield. In such case, it can include the penetration of computers or networks, denial-of-service (DoS) attacks against computers and/or networks, and the manipulation of the adversary's information sources so to control or condition its thinking;
2) the delivery of an attack by State A against State B by using computers and/or network-based capabilities;
3) the confrontation between States in which cyber attacks reach the threshold of an attack or in which cyber activities take place during an armed conflict. For a cyber attack to be compared as armed attack, it has to be aimed at undermining the functioning of a digital information system or network for political or national security reasons.

For the seek of this dissertation, the author will adopt the definition set forth by the ICRC in its 2019 Report, that defined cyber warfare as "operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means or methods of warfare in the context of an armed conflict."[117]

With regard to 'cyber war', instead, the term refers to "a sustained computer-based cyberattack by a state, state-owned organization [...] or state-sponsored organization against the IT infrastructure of a target state."[118]

---

[116] Erwin Orye and Olaf M. Maennel. "Recommendations for Enhancing the Results of Cyber Effects" in *2019 11th International Conference on Cyber Conflict: Silent Battle*, eds. by T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (Tallinn: 2019 NATO CCD COE Publications, 2019), p. 4.

[117] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Recommitting to the Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, ICRC, 2019, p. 26.

[118] ibid., p. 2.

Once the attempt to define the terminology pertaining to the cyber realm has been made and the characteristics of cyber attacks have been highlighted, it is necessary to establish what are the tools that can be used to conduct such type of cyber operations.

4.2 Cyber weapons and their effects

Cyber attacks can be conducted through the use of different tools, also known as cyber weapons. Despite of the frequent use of the term 'cyber weapon', and as in the case of the majority of the terms of the cyber realm, no agreed definition of cyber weapon has been reached so far. The 2019 edition of the *NATO Glossary of Terms and Definitions*, for instance, does not include any definition of cyber weapon, neither does the US DoD Military and Associated Terms.

Stefano Mele, Italian lawyer and cyber expert, has provided with an attempt of definition for this new type of weapons:

> "A cyber weapon is [an] appliance, device or any set of computer instructions designed to unlawfully damage a computer or telecommunications system having the nature of critical infrastructure, its information, data or programs contained therein or pertaining there to, or to facilitate the interruption, total or partial, or alteration of its operation."[119]

This definition is considered to be legally valid and qualifies a cyber weapon for its capability both to cause the loss of human life and to damage critical infrastructure.

In the context of a cyber weapon that could potentially lead to the breakout of a conflict, instead, Mele came up with a different definition. Tracing a line between cyber weapons used for purposes such as cybercrime or cyber espionage and those used for cyber attacks is fundamental, indeed. Stefano Mele took into account three key factors, namely the context, the purpose, and the tool/mean. In the context typical of an act of cyber warfare,[120] with the purposes of causing physical damage to people or objects - directly or indirectly - or of

---

[119] Pierluigi Paganini, "The Rise of Cyber Weapons and Relative Impact on Cyberspace," *Infosec*, 5 Oct. 2012, available at https://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/#gref

[120] With context 'typical of an act of cyber warfare', Stefano Mele refers to the context of a conflict among actors, these being national or non-national in character, characterized by the use of information systems, and aiming at achieving, or keeping, or defending something that is considered to have either a strategic or an operative and/or tactical advantage. (Stefano Mele, "Legal Considerations on Cyber-Weapons and Their Definition," *Journal of Law & Cyber Warfare* Vol. 3, No. 1 (2014) p. 58.)

sabotaging or creating damage to the information systems of the target, and performed by using the information systems, a cyber weapon could be defined as:

> "A part of equipment, a device, or any set of computer instructions, used in a conflict among actors both National and non-National, with the purpose of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject."[121]

Furthermore, in the classification of cyber means, a malicious code could be identified as a 'weapon' not only for its intrinsic nature, but also for the effects it is designed to produce. Therefore, the purpose for which a certain cyber tool is created is very relevant for its classification as a 'weapon'. In the words of Louise Arimatsu,

> "[...] only if it is established that a malicious code possesses an offensive capability and there is an intention to use it in a manner which comports with its offensive capability might the malware be deemed a 'cyber-weapon'. Accordingly, it is both the offensive capability of the malicious code and the intended outcome or effect produced by that code that transforms it into a weapon [...]."[122]

Dorothy Denning, member of the Naval Postgraduate School, distinguishes between cyber weapons designed for offence purposes only - used to attack and cause harm-, those that are designed for defence purposes only - used mostly to protect against an attack-, and the dual-use cyber weapons - used both for offence and for defence purposes. In her classification, Denning focuses on the type of malware and its use. Cyber weapons designed for offence purposes, which is the category of major interest for this dissertation, can be viruses and worms, as well as Trojan horses or denial-of-service attacks.

To sum up, cyber tools that fit the above-explained criterias can be considered cyber weapons, and represent the means through which one is able to carry out a cyber attack. Cyber weapons are designed to cause the corruption of the hardware, or of the software of the targeted system - through viruses and worms, for example-, or the collapse of the system by flooding it with information.

With regard to the corruption of the hardware of a system, an example of such type of attack is that of 'chipping'. Chipping refers to the integration of computer chips that are already damaged or corrupted into the hardware of the targeted system.

---

[121] Stefano Mele, "Legal Considerations on Cyber-Weapons and Their Definition," *Journal of Law & Cyber Warfare* Vol. 3, No. 1 (2014): p. 58. Accessed 30 January 2020. www.jstor.org/stable/26432559.

[122] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations" in *2012 4th International Conference on Cyber Conflict*, eds. C. Czosseck, R. Ottis, K. Ziolkowski (Tallinn: 2012 NATO CCD COE Publications, 2012), p. 98.

Malwares, instead, are used for the purpose of corrupting the software of the targeted system. A malware is a malicious software, such as a virus or a worm, that breaches a network by taking advantage of one or more of its vulnerabilities. A virus is a self-replicating program that carries a payload - or code - which will corrupt or delete computer data on the targeted computer. In order to work, the virus has to attach itself to a legitimate program, that will be corrupted and/or modified and that will be the mean through which the virus will spread to other programs on the targeted computer, and if the computer is connected to a network, it will probably spread to other computers as well. A worm, instead, replicates itself in other computers without modifying other programs. In fact, a worm is not meant to attach itself to programs so to modify them, since its purpose is that of capturing the address of the targeted computer to resend messages throughout the system attacked in order to cause it to slow down, and possibly to crash. Furthermore, while a virus needs human intervention to spread, a worm does it automatically. Both viruses and worms can be hidden in the so-called Trojan horses, that appear as innocuous code fragments, but that instead cover up a harmful program or allow an external user to have access to the targeted computer from remote. Types of Trojan horses are logistic bombs or time bombs, which are designed to carry out an attack in specific circumstances or at a certain time.

Attacks that are meant to cause the collapse of a system by flooding it with information, or the so-called 'flood attacks', can be carried out through Denial of Service (DoS) attacks. Such attacks do not need to penetrate into the system, since their purpose is to literally inundate the targeted computer, network or system with a high number of calls, messages, requests, or more generally with traffic, so to overload it. Once overloaded, the target will not be able to fulfill legitimate requests, and the attack will force the target to shut down. The perpetrators of the attack can also carry it out by using multiple compromised devices organized in 'botnets.'[123] In this case, the attack would be called distributed-denial-of-service (DDoS) attack.

Viruses, worms, logistic and time bombs, as well as Trojan horses can be installed in a computer in different ways: through chipping, hacking, phishing, or through an hard drive, for instance.

---

[123] A 'botnet', or 'robot networks', is a network of devices that has been corrupted or infected with a malicious software, such as a virus for instance. Botnets are frequently the source of spam.

The spectrum of targets for a cyber weapon is quite wide. Generally, a cyber weapon targets the critical infrastructure of a State or its vital system. Examples of possible targets are industrial control systems, such as plants for energy production; electric power supply grids; electronic national defense systems; military air traffic controls or airspace control systems; hospitals or government control systems.[124] More in detail, by launching a cyber attack against control systems of critical facilities, for instance, the management system of a nuclear plant could be compromised and it could cause the alteration of the production processes as well as the exposure of entire areas to the risk of being destructed.

The management systems of electricity grids are vital for the functioning of a state; should these be the target of a cyber attack, the supply of electricity to the country would be halted and consequently cause a total black out of the activities of a state - such as hospitals, public transportation, telecommunication services. The consequences could be devastating.

By hacking the electronic national defense system of a State, instead, the attacker could control the conventional weapons of the country attacked and launch missiles against the same state or another state.

As can be understood, an attack against the military or civilian air traffic control or against the airspace control systems could have devastating consequences and cause the loss of human lives as well as the destruction of objects. Furthermore, it is important to consider the fact a part from hitting their primary targets, cyber attacks can damage also third objects or systems. Unpredictably, a cyber weapon could hit other systems or networks that were not considered as targets of the attack. An evaluation of the effects of a cyber attack is fundamental for establishing when a cyber attack can amount to use of force or armed attack.

4.2.1 The taxonomy of cyber effects

When analyzing the effects of cyber attacks, it is important to keep in mind that the terms kinetic and lethal and non-kinetic and non-lethal should not be equated. Both cyber operations and cyber attacks can have physical and cognitive effects, as well as lethal outcomes. Cyber attacks, in fact, are able to degrade, disrupt, deny or even destroy

[124] Pierluigi Paganini, *The Rise of Cyber Weapons and Relative Impact on Cyberspace*.

information technology-dependent infrastructures and data.[125] However, the effects of malicious cyber operations or of cyber attacks are not always limited to their target. On the contrary, they can manifest in various ways - directly or indirectly- and can be classified as follows.

The so-called first-order effects are those effects that manifest within the target - IT system - of the initial malicious cyber operation or of the initial cyber attack. Based on a single cyber operation or attack, first-order effects can cause further effects identified as 'cascading effects'. Cascading effects can be compared to a cause-effect chain, and when they take place within the same IT system targeted by the initial malicious cyber operation or cyber attack, they are considered to be first-order effects.

Cyber operations and cyber attacks can have second-order effects, that is to say, effects that manifest outside the targeted IT environment. As Orye and Maennel explain, "[t]hose effects represent the indirect effect caused by system failures triggered by the cyber operation [...]."[126]

Lastly, a cyber operation or a cyber attack can have third-order effects, that are usually considered to be long-term. Examples can be the way in which the cyber operation or cyber attack has influenced international relations, or the change of behavior in institutions, or even changes in societal behavior, or the financial impact of the initial cyber operation or attack. In short, they represent the overall results of the first-order effects taken in conjunction with the second-order effects. Third-order effects can have a profound impact on strategic and political levels.

Second-order and third-order effects are potentially more dangerous than first-order effects, and the relationship between the various systems affected by the initial cyber operation or cyber attack should always be taken under consideration when evaluating the outcome of such operations and attacks, especially when a legal evaluation of the happenings is made.

Erwin Orye and Olaf M. Maennel introduce a taxonomy of cyber effects from the perspective of nation-states in their "*Recommendations for Enhancing the Results of Cyber Effects"*, published for the 2019 11th International Conference on Cyber Conflict, organized by the

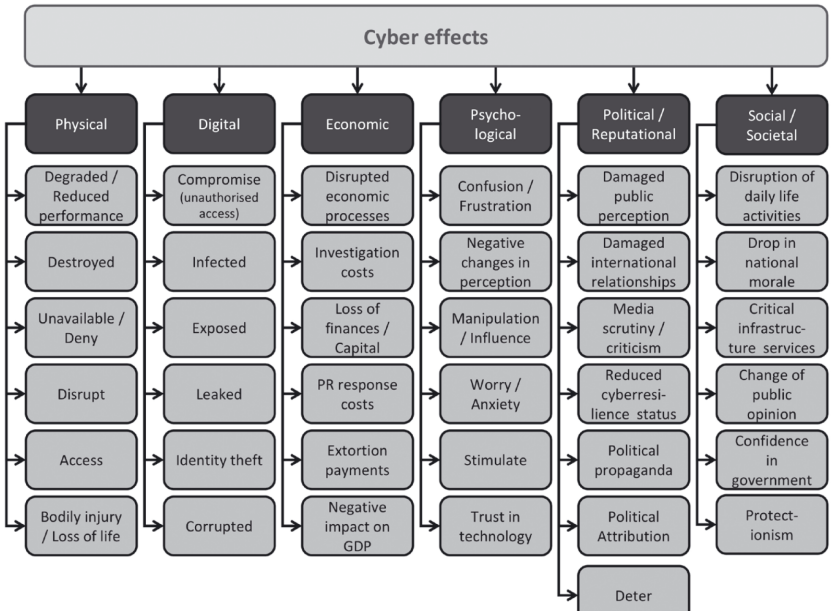
---

[125] Erwin Orye and Olaf M. Maennel, "Recommendations for Enhancing the Results of Cyber Effects," p. 12.

[126] ibid., p. 5.

NATO CCD COE. Such taxonomy displays the cause-effects of a cyber operation, evaluating also political and economic outcomes, for instance.

Figure 1: Taxonomy of cyber effects



Source: Erwin Orye and Olaf M. Maennel. "Recommendations for Enhancing the Results of Cyber Effects" in *2019 11th International Conference on Cyber Conflict: Silent Battle*, eds. by T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (Tallinn: 2019 NATO CCD COE Publications, 2019) p. 13.

Understanding all that a cyber operation or cyber attack encompasses is fundamental for the purpose of creating a solid legislation for the cyber domain. Adopting an effect-based approach in the evaluation of malicious cyber operations from a legal perspective seems to be the fairest way to deal with the new domain, so to punish breaches of the law on the use of force and to regulate cyber attacks during armed conflicts. Taking into consideration only the nature of the attack when establishing if a malicious cyber operation or cyber attack reaches the level of use of force or when it is used in a military operation is thought to be reductive and to lead often to an incomplete analysis.

In the second chapter of this dissertation, the theoretical concepts explored in this first chapter - such as the interpretation of the use of force, of the right to self-defence and the rules regulating the conduct of hostilities - will be applied to what we have discovered a malicious cyber operation or a cyber attack is.

The questions that will be addressed are the followings: when does a cyber operation reach the threshold of threat or use of force under Art. 2(4) of the United Nations Charter? When

can a cyber attack be considered as armed attack under Art. 51 of the UN Charter, and thus trigger the right of individual or collective self-defense? And lastly, when is a cyber operation considered as an attack under International Humanitarian Law?

CHAPTER 2

Cyber Operations and the *jus ad bellum*

The regulation of cyber operations under International Law and International Humanitarian Law carries several difficulties. From the lack of official and internationally agreed definitions concerning the cyber realm to different perceptions of the threats that can be posed by the new domain, the road to the formulation of a solid legal instrument capable of encountering agreement amongst the international community and of regulating cyber operations is still long and tortuous. Different perspectives have been proposed to face the dilemma of applying 'old laws' to a new domain. They range from a strict application of the law for which what is not prohibited is permitted, to a wider interpretation of the law that treats it as a set of ever-evolving norms that are not only part of treaty law but have also become customary in character and should be applicable to this new domain. What is certain is that, due to the rise in usage of cyber operations - both offensively and defensively- and to the strengthening of national and regional cyber capabilities across the globe, it is in the best interest of each national and supranational entity of the international community to find agreement and to enact a legally binding international instrument on the conduct of such operations. Attempts have been made, but have not been successful yet. Nevertheless, the increase in forums - such as the annual International Conference on Cyber Conflict (CyCon) organized by the NATO CCD COE - and debates on the subject, together with the publication of reports - as the ones published by the UN Group of Governmental Experts (GGE) on cyber-security related topics- have brought to the delineation of the most common and spread ideas on how the issue should be regarded and, most importantly, dealt with from an international law perspective.

In this Chapter, we will discuss firstly how the prohibition on the use of force contained in Article 2(4) of the UN Charter and its customary international law counterpart could be applied to cyber operations; secondly, we will discuss when a cyber operation could be considered to be reaching the threshold of 'armed attack' and thus trigger the right of self-defence contained in Article 51 of the UN Charter.

1. Cyber Operations and the 'use of force' paradigm

As argued in Chapter 1, the interpretation of the prohibition on the use of force still leaves a number of interpretative quandaries open. The findings on the discussion concerning the meaning of Article 2(4) of the UN Charter in Chapter 1 can be summarized as follows: all the uses of force exercised by *de jure* or *de facto* organs of a state against another state - thus, in their international relations - is prohibited. Additionally, the use of force needs to be undermining the territorial integrity and/or the political independence of a sovereign State, or if need be, against the purposes of the United Nations.

With regard to the meaning of 'force' it has been found that the most common interpretation of the wording of Article 2(4) of the UN Charter, of the UN Charter as a whole, and of the *travaux préparatoires* of the same Charter, bring to the conclusion that for 'force' we intend 'armed' force. However, both international jurisdiction and state practice have enlarged the meaning of 'force' so to include also actions that do *not* involve necessarily a state's direct use of armed force. In the *Nicaragua* case, in fact, the ICJ found that the arming and training of the *contras* by the United States of America was to be considered use of force. On the contrary, the mere supplying of funds to the *contras* was not to be considered use of force, but a breach of the principle of non-intervention, instead. In the aforementioned judgement, in order to make a distinction in between those actions amounting to a state's *indirect* use of force and those actions that simply do not amount to a use of force, the ICJ distinguished between the 'most grave forms' of use of force and the 'less grave forms'. Instead of looking at the nature of the action *stricto sensu*, the Court focused on the 'scale and effects' of the action, that has to be conducted by or otherwise be attributable to a State. As it has been argued and will be further argued, the 'scale and effects' criterion captures both the quantitative and qualitative factors that should be analysed when determining in what cases an action amounts to use of force.

Notwithstanding the demand for economic coercion to be considered use of force, advanced mostly by developing states, the international community rejected the proposal. Economic coercion is, in fact, prohibited under the UN General Assembly *Declaration of Friendly Relations*, but it is not considered a breach of Article 2(4) of the UN Charter.

The lawfulness of other uses of force has been challenged in light of the prohibition itself. The use of force to protect nationals abroad - used by Israel in 1976 and by the US in 1983 - received international support because it was found not to be contrary to the purposes of the United Nations, for instance. Uses of force in pursuit of self-determination, instead, received no support with regard to their lawfulness when such uses of force were outside the context of decolonization or illegal occupation. For what concerns the use of force in pursuit of democracy, it is not considered to be lawful: the fact that, in exceptional cases, the United Nations may have the power to authorize the resort to force to restore a democratic government should not be extrapolated and transformed into a right of unilateral intervention by States.

The shadows surrounding the definition of 'force' leave space for doubts, which are often intentionally left unresolved and open for further interpretations. This is due to the fact that, in the opinion of the UN General Assembly and of the International Court of Justice, the provisions of the Charter should be regarded as dynamic, and thus capable of changing over time with State practice.

This brings us to the first questions that will be addressed in this Chapter, that are: should *de lege lata* in question be applicable to operations conducted in the cyber domain? Moreover, can a cyber operation be considered use of force in breach of the prohibition contained in Article 2(4) of the Charter? If so, when does a cyber operation reach the threshold of threat or use of force under Article 2(4) of the United Nations Charter?

1.1 Old Laws for new uses of force?

With regard to the applicability of *de lege lata* surrounding the prohibition on the use of force to cyber operations, there is broad agreement on the fact that both Article 2(4) of the UN Charter and its customary international law counterpart, as *jus cogens*, should be applicable to cyber operations.

Furthermore, unless the international community is prone to adopt a "*de novo* scheme for assessing the use of inter-state coercion, any justification or condemnation of [cyber

operations] must be cast in terms of the use of force paradigm."[127] In Michael N. Schmitt's opinion, shared by the author of this dissertation, it is not necessary to craft a new legal scheme to deal with the cyber realm, but to determine how to address actions and activities that were not contemplated at the time in which the UN Charter was created. In 1945, the drafters of the Charter simply could not have envisaged the advent of cyber activities and thus, they could not have seen beyond their knowledge of the notion of 'force', which was that of 'armed force'. However, it was decided to leave the concept of 'force' blurry so that it could evolve together with the change of times. In support of this view, as it has been stated already, the *Nicaragua* judgement suggested that other forms of 'force' distinct from 'armed force' could be identified. Then, the fact that cyber operations are not carried out through traditional means should not represent an obstacle when it comes to their regulation under international law, and most importantly, under the prohibition on the use of force. Certainly, policy concerns may drag some States towards the will to regulate cyber operations within the existing legal framework and some others towards the opposite direction. However, it should be considered that the international security framework established by the UN Charter would surely be best affected by thinking about it as being inclusive, that is, capable to enlarge its scope with the advances and the progress of our times. In the words of Michael N. Schmitt, "[...] to the extent that treaty prohibitions have any deterrent effect, inclusivity would foster shared community values,"[128] such as the maintenance of international peace and security - which can be translated, on a larger picture, in the preservation of humankind -, and human dignity - and thus the respect for human rights. If the opposite reasoning was to be made, that is to say, if the Charter's provisions were not to be regarded as inclusive, many uses of force that belong to the new era and are brought about by the advances in technology and by the introduction of new and more sophisticated military tools could be left uncondemned.

Another argument in favor of the application of *de lege lata* to cyber operations is supported both by the CCD COE International Group of Experts and by scholar Nils Melzer. In their studies, they highlight that the ICJ clearly stated that both Article 2(4) and Article 51 of the

---

[127] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: thoughts on a normative framework," *Columbia Journal of Transnational Law* Vol. 37 (1998-99): p. 913. https://ssrn.com/abstract=1603800

[128] ibid., p. 919.

United Nations Charter apply to "any use of force, regardless of the weapon employed."[129] Such statement accurately reflects customary international law. Hence, the fact that an operation is conducted through the use of a computer, instead of a more traditional weapon, should not be an obstacle for an operation to be condemned as a use of force. As Nils Melzer states, "it is relatively uncontroversial that cyber operations fall under the prohibition of article 2(4) of the UN Charter once their effects are comparable to those likely to result from kinetic, chemical, biological or nuclear weaponry."[130] As discussed in Chapter 1, cyber operations can be carried out through the use of both defensive and offensive tools. In the latter case, such tools are designed with the intention of causing death and/or injury to persons, and/or destruction of objects as well as of infrastructure, regardless of the nature of the destruction - be it physical damage or functional harm. An example of a cyber operation reaching the threshold of use of force within the meaning of Article 2(4) of the UN Charter could be the disablement of an airport air traffic control during bad weather conditions, action that could result in severe injury, death *and* destruction. In this case, even though the operation would not be carried out through traditional means, as could be the launching of missiles against a civil airplane, the effects of the kinetic and of the cyber operation could potentially lead to the same results: injury and/or death of people, as well as destruction of objects.

Certainly, the application of 'non-violent' tools and methods that are equivalent both for their intent and for their purpose to violent/kinetic tools, and that cause similar consequences, cannot circumvent the prohibition on the use of force expressed by the Charter. It is sufficient to think about the effects of a cyber operation that incapacitates the control systems of a nuclear power station causing its meltdown, for instance, to understand that the application of 'non-violent' means should not obstruct their condemnation under international law and, in particular, under the prohibition on the use of force if their intent and results are violent. In this context, it is important to keep in mind also that Article 2(4) prohibits the use of force in inter-state relations notwithstanding their duration or of their magnitude. This means that even minor actions manifesting inter-state force fall under the aforementioned provision, regardless of the possibility to classify them also as acts of aggression or as armed attacks.

---

[129] *Legality of The Threat or Use of Nuclear Weapons*, *Advisory Opinion*, ICJ Reports 1996, para 39, p. 244.

[130] Nils Melzer, *Cyberwarfare and International Law*, p. 7.

For all the has been discussed above, then, we can draw the conclusion that "the use of force line must lie somewhere between economic coercion and the use of armed force."[131] What is still unclear is how to precisely draw the line of demarcation for which a certain action amounts or does not amount to a use of force in the cyber context. In the words of Nils Melzer, "[t]ruth is that cyber operations, almost always falling within the grey zone between traditional military force and other forms of coercion, simply were not anticipated by the drafters of the UN Charter."[132] Nowadays, state practice and the international jurisprudence have failed to identify solid criteria on how to classify those cyber operations that do not cause death, injury, or destruction but that could still be regarded as a use of force under Article 2 (4) of the UN Charter.

Having stated that *de lege lata* in the area can and should be applicable to cyber operations, a first attempt to solve the dilemma on *how* it applies could be that of starting from the roots of the prohibition on the use of force and try to solve all the interpretative quandaries that emerge when applying the rule to cyber operations.

In order for a cyber operation to be object of applicability of Article 2(4) of the UN Charter and of its customary international law counterpart, it has to meet a set of criteria required by the prohibition itself. Firstly, for a cyber operation to be considered as a use of force, it must be attributable to a State, since armed groups or civilians by themselves do not fall within the scope of the prohibition. Secondly, the cyber operation in question needs to amount to a threat or use of 'force', as explained above. Lastly, the cyber operation has to be conducted by State A against State B, that is, in their international relations.

For what concerns the first criterion, this dissertation will not discuss rules on State Responsibility nor problems of attribution of a cyber operation to a State. This is not to underestimate the difficulty that the new domain and its intrinsic intangibility pose to attribution, but simply because it is outside the scope of this dissertation. For this reason, in our analysis, we will assume that the cyber operation in question has been successfully attributed to a State.

Concerning the second criterion, the classification of a cyber operation as a use of force will be a matter of discussion thereafter.

---

[131] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: thoughts on a normative framework," p. 914.

[132] Nils Melzer, *Cyberwarfare and International Law*, p. 9.

Finally, as it has already been said, the prohibition applies only in State's international relations, which means that it is applicable if State A mounts a cyber operation reaching the threshold of use of force against State B, but not if State A addressed the cyber operation against a group or an individual inside its territory, as long as such cyber operation does not affect State B's territorial integrity or political independence. Therefore, whether or not a particular cyber operation falls within the scope of Article 2(4) of the United Nations Charter, having satisfied the criteria explained above, depends ultimately on how we understand the nature of armed force itself, that is to say, on which of the three analytic approaches we choose to use in order to establish what is the determinative factor that qualifies an action as 'armed force'.[133]

1.2 Cyber Operations as (armed) force

Although fundamental, a coercive intention is not by itself enough to classify a cyber operation as a use of 'armed' force. Contrary to other forms of coercion that do not reach the threshold of use of force - diplomatic and economic coercion, for instance -, armed force is understood as a severe form of intervention that carries the intention of the coercive State to violate militarily and politically the sovereignty of the victim State, influencing its internal and/or its external affairs. However, the mere coercive intention is not a satisfying and complete criterion to determine whether a cyber operation - or any other type of coercive action - amounts to use of force. Debates among scholars over how *jus ad bellum* applies to cyber operations have brought to light three leading approaches that attempt to determine when a cyber operation can be classified as use of 'armed' force, that are 1) the instrument-based approach; 2) the target-based approach; and 3) the effect-based approach.

At least since the UN Charter was promulgated, the use of armed force paradigm has been instrument-based.[134] This approach focuses on the physical characteristics of the instrument used to carry out the coercive action, i.e., weapons, in what it distinguishes the action itself from other forms of coercion, such as the economic one or the political one. Such

---

[133] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 46.

[134] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: thoughts on a normative framework," p. 909.

approach, therefore, determines whether or not the use of force paradigm has been breached depending on the type of coercive instrument used to reach the coercive State's objective. Diplomatic and economic instruments can breach the principle of non-intervention, while military instruments can breach the prohibition on the use of armed force. However, the instrument-based approach has been strongly criticized since it would lead to the conclusion that, for their physical characteristics, cyber operations could never be identified as a use of force under Article 2(4) of the Charter, even in the case in which they cause physical damage, in spite of the fact that certain digital codes, depending on their payload - destructive or non-destructive -, have been classified as (cyber) weapons by a large share of international scholars. Furthermore, it is important to take into account that not all coercive actions involving armed force are contrary to the community values preserved by the United Nations Charter, and even when they are, they do not always result in greater damage or violence than other forms of coercion. As a matter of fact, "a temporally and spatially limited border incursion is probably a lesser threat to either international peace and security or the right of states to conduct their affairs free from outside interference than was the 1973-74 Arab oil embargo."[135] Nevertheless, the instrument-based approach to the use of force paradigm would proscribe the first case, but not the second one. As explained by Oona A. Hathaway et al., the UN Charter actually provides support for the approach in question, on the one side because its Article 41 defines the "complete or partial interruption of [...] telegraphic, radio, and other means of communications" as actions that do not involve the use of armed force.[136] On the other side, the *Definition of Aggression* of the United Nations General Assembly lists in its Article 39 a number of actions that would be considered aggression, all of which are carried out through military tools, i.e. traditional weapons, or force, implicitly supporting the instrument-based approach as well. If one should focus on the advantages of applying such approach, the main one would surely be the simplicity of its application, since it is quite easy to identify what constitutes a use of military weapon. However, the implicit intent of the legal framework of the prohibition on the use of force is that of avoiding the *consequences* caused by the usage of military tools and weapons, that are the injury or death of people, and the damage or destruction of objects. As argued by Michael N. Schmitt:

---

[135] ibid.

[136] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel,"The Law of Cyber-attacks," *California Law Review* Vol. 100, No. 4 (August 2012): p. 846.

> "[b]ecause force represents a consistently serious menace to intermediate and ultimate objectives [such as the preservation of the community values explained above, i.e., the maintenance of peace and security, the safeguard of human dignity, etc.] the prohibition of resort to it is a relatively reliable instrument-based surrogate for a ban on deleterious consequences."[137]

Therefore, what should be the focus of the prohibition are the consequences caused by coercive actions rather than the means through which they are perpetrated. Indeed, cyber operations can potentially inflict catastrophic harm, even absent the employment of traditional military weapons. For this reason, many scholars have rejected the criterion of defining uses of armed force by applying the instrument-based approach, describing it as outdated.

The target-based approach, instead, focuses on the target of the operation. Therefore, it is argued that a cyber operation reaches the level of a use of armed force when it is conducted against sufficiently important computer systems, as the ones concerning the national critical infrastructures (NCIs) of a State, regardless of the nature of the operation or of the effects that it may have. However, it is important to keep in mind that the infiltration of a national critical infrastructure through a cyber operation should not be equated with the direct or indirect causation of harm. Cyber exploitation tools, for instance, penetrate a system for exploitation purposes - as the stealing of data -, but do not carry a destructive payload within them and are not intended to cause harm to the system they infiltrate, nor to the infrastructure and/or services that rely on such computer system. Furthermore, as argued by the NATO CCD COE International Group of Experts in the *Tallinn Manual 2.0*, cyber operations targeting other computer systems different from national critical infrastructure could raise to the level of use of force as well, but they would be cut out by the approach in question. Hence, the target-based approach is likely to condemned cyber operation clearly not raising to the level of use of force just for the mere fact that they are conducted against national critical infrastructures, but not to condemn cyber operations that have destructive capacity just because they are not directed against NCIs.

Lastly and most importantly, the effect-based approach is the approach that has received broader support by the international community and that is thought to be the most suitable for the regulation of cyber operations in the context of the *jus ad bellum*. Such approach classifies cyber operations by focusing on the effects that they may cause. In this

---

[137] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: thoughts on a normative framework," p. 911.

regard, the difficulty in its application lies in the fact that cyber operations span "the spectrum of consequentiality."[138] Their effects, in fact, range from simple inconvenience to death or injury of persons, and to damage or destruction of objects. They can affect, directly or indirectly, social, economic and physical or psychological security. Hence, the use of force demarcation line must be placed somewhere in between economic or diplomatic coercion and the use of force reaching the threshold of armed attack. There is broad agreement over the fact that, for a cyber operation to be considered as reaching the level of use of armed force, it has to have destructive effects on persons and/or objects. Different versions of the effect-based approach measure the gravity of the damage inflicted by relying on a set of different criteria, that range from the severity of the harm caused alone, to the length of the cause-and-effect chain triggered by the initial cyber operation itself and the ultimate harm.[139] However, there is broad agreement over the fact that any cyber operation that causes or that is likely to cause the same damage as the one usually produced by the use of kinetic weapons should be considered use of force. As Harold Koh, then Legal Advisor of the US State Department, stated at USCYBERCOM in 2012, "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force."[140] By changing cognitive approach, and thus by focusing on the consequences caused rather than on the means through which actions are carried out, cyber operations fit more easily within the existing international legal framework regulating the resort to force in times of peace, that is to say, the *jus ad bellum*.

In support of this view, shared by the author of this dissertation, and as already mentioned in Chapter 1, the treatment of biological and chemical weapons under Article 2(4) demonstrated that armed force should not be equated only to means that are kinetic in nature. Furthermore, this view cannot be contested by Article 41 of the UN Charter since, as discussed in Chapter 1 when displaying all that the definition of cyber operations encompasses, cyber operations and in particular cyber attacks can serve objectives and have effects that go way beyond the

---

[138] ibid., p. 912.

[139] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber-attacks," p. 847.

[140] Harold Koh, "International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012", *Harvard International Law Journal Online* Vol. 54, (December 2012): p. 4.

mere interruption of 'telegraphic, radio, and other means of communication', which of course would not be regarded as use of force.

The *Tallinn Manual 2.0* adopts the same view, and states in its Rule 69 on the *Definition of use of force* that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force." Accordingly, one category of cyber operations is smoothly dealt with. Cyber operations, more precisely cyber attacks, specifically intended to cause *direct* injury or death to persons, and/or physical damage to or destruction of property would be classified as use of armed force and thus would be subject to the prohibition. Having reached this conclusion, there is still one question to be answered: how should cyber operations that do *not* cause *directly* injury or death of persons, and/or physical damage to or destruction of property be dealt with under Article 2(4) of the Charter?

In order to determine whether a cyber operation can amount to use of force even when it does not cause direct harm, we will refer to the list of determinative factors that Michael N. Schmitt elaborated in 1999 in *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*. Such factors have been discussed for two decades amongst the international community and, although considered non-exhaustive, have helped the shaping of more solid criteria to solve the use of force dilemma that concerns the regulation of cyber operations. They are thought to be very helpful in determining the 'scale and effects' of cyber operations that trigger detrimental consequences, non-physical in nature, but that sufficiently resemble those triggered by a kinetic use of force. The criteria developed by Schmitt were originally six, but have been expanded to eight in the commentary of Rule 69 on the 'Definition of use of force' of the *Tallinn Manual 2.0*, of which Michael N. Schmitt is the General Editor. The factors in question are the followings: severity, immediacy, directness, invasiveness, measurability (of effects), presumptive legitimacy, with the recent addition of military character, and state involvement.

With regard to Severity, Schmitt argued that it had to be one of the criteria because physical well-being usually is on the top of the hierarchical pyramid of human needs. Since the use of armed force represents a threat of physical injury or destruction of objects to a much greater extent than economic or diplomatic coercion, a cyber operation whose effects resemble those of kinetic armed force has to be considered use of force as well. Cyber operations that

generate mere inconvenience will not be considered as such. The NATO CCD COE International Group of Experts pushes forward the definition of the criterion by saying that in between the two situations displayed above, that are extremes, "the more the consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operations as a use of force."[141] Furthermore, the International Group of Experts recognized that other factors, such as the scope, the duration and the intensity of the consequences will have great relevance on the estimation of the severity of the action.

The second criterion for our analysis is that of immediacy. As Schmitt explained, the consequences of a use of armed force are more imminent in their manifestation, *vis-à-vis* the consequences caused by other forms of coercion. As a result, more imminent the consequences manifest, the less time will States have to respond by seeking peaceful accommodation of the disputes or to limit the harm expected from the use of armed force in question. Hence, States are surely more concerned by actions entailing imminent consequences than about the opposite. As a result, cyber operations that produce imminent effects are more likely to be considered use of armed force than those operations that take weeks or months to manifest them. What the author of this dissertation finds unclear regarding the criterion of immediacy is the fact that, as discussed in Chapter 1, cyber operations trigger first-order, second-order and third-order effects. Taking into account that first-order effects are considered to be those inside the targeted IT system, that second-order effects are considered to be those that manifest outside the targeted IT system but directly connected to it, and third-order effects are usually long-term and on a macroscale - such as political, social effects -, to what order of effects should we be referring to? In the opinion of the author, third-order effects should not be regarded as they are long-term and operate on macro-societal, or macro-political, or macro-economic changes, neither should first-order effects since they will not directly result in the killing of people or in the damaging and/or destruction of property. What should be the focus, then, are second-order effects, that is to say, the tangible effects caused by the initial cyber operation targeting a certain IT system, but outside the IT system itself. Furthermore, time bombs - a category of cyber attacks, in particular of Trojan horses -, are purposely designed to produce their effects only at a certain and precise time, that could be months away from the installation of the time bomb itself. In

[141] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 334.

the opinion of the author, if the criterion of immediacy was to be applied strictly, time bombs could not be regarded as a use of force, since their effects can be very dilated in time. However, their degree of severity could be important enough to have them characterized as a use of force. Unfortunately, the literature on this subject does not provide elements to better interpret the concept of effects in relation to the immediacy criterion, leaving these questions open for further reflection and discussion.

For what concerns the third criterion, directness, Schmitt argues that "the consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion [...]."[142] While immediacy measures the temporal aspect of the consequences caused by the action in question, the criterion of directness analyzes the chain of causation. In the *Tallinn Manual 2.0* it is argued that, in the case of economic coercion, "[t]he casual connection between the initial acts and their effects tends to be indirect [...]. In armed actions, by contrast, cause and effects are closely related."[143] For this reason, those cyber operations whose consequences or effects are clearly linked to their cause - the initial cyber operation itself - have a higher chance to be classified as uses of force than those cyber operations that are not directly connected to their effects. The analysis of the NATO CCD COE International Group of Experts, however, does not come without flaws. Marco Roscini, for instance, argues that directness is not automatically a characteristic strictly related to the nature of the use of force. He recalls the *Nicaragua* judgement, in which the ICJ stated that not all uses of force involve the coercive State's direct use of armed force. In that case, the mere arming and training of the contras sufficed to classify the actions of the United States as a use of force. Furthermore, and as partly discussed for the criterion of immediacy, cyber operations often manifest their effects *indirectly*. In fact, the intended effects of a cyber operations are often the results of the first-order effects, that is to say, of the "alteration, deletion, or corruption of data or software or the loss of functionality of infrastructure."[144]

The fourth factor is that of invasiveness. Michael N. Schmitt explains that what distinguishes armed force from other forms of coercion is that the action that causes the harm usually happens inside the target State's borders or anyway into the targeted State's area of

---

[142] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: thoughts on a normative framework," p. 914.

[143] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 334.

[144] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 48.

sovereignty, whereas in economic coercion, for instance, the act usually takes place beyond the targeted State's borders. As a consequence, the degree of intrusion into State sovereignty is higher in the former case than in the latter, and as such, it is more likely to threaten international peace and security. Transposing such argument to cyber operations, the criterion "refers to the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of [the targeted] State."[145] For such reason, if a highly secured cyber system were to be penetrated, the cyber operation would be perceived as more intrusive. As explained in the *Tallinn Manual 2.0*, cyber operations targeting specifically the domain name - 'websitename.*it*' in the case of Italy or 'websitename.*us*' in the case of the United States for instance - are considered to be more invasive than cyber operations targeting a non-State specific domain extension, as 'websitename.*com*' or 'websitename.*org*'. However, such criterion has to be considered cautiously in that not all invasive cyber operations are uses of force. Cyber espionage, for example, is highly invasive but the cyber tools used for it often do not carry a destructive payload, since its ultimate goal is that of stealing information and not that of disrupting the system intruded. On the contrary, cyber attacks conducted through the so-called 'flood attacks' are not invasive but their ultimate goal is surely disruptive. In this case, the attackers need not penetrate into the target system to achieve the desired disruption, since the targeted system is inundated by the outside through 'botnets' or by flooding the target system with requests.

For what concerns the fifth criterion, that of measurability of effects, Schmitt argues that the consequences of armed coercion are usually easier to identify than those caused by other forms of coercion. For this reason, it is easier to condemn an act of armed force rather than another act of coercion. However, in the cyber domain, consequences are less obvious than in traditional uses of armed force. Hence, as expressed by the NATO CCD COE International Group of Experts, "the more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of use of force."[146] This means that the more the elements of a certain cyber operation that can be evaluated - such as the amount of data that were corrupted

---

[145] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 334.

[146] ibid., p. 335.

or exfiltrated, how many servers were disabled by the operation, etc. -, the more it is likely that the cyber operation in question will be categorized as use of armed force.

The sixth criterion of our evaluation is that of presumptive legitimacy, which is connected to the principle that what is not explicitly prohibited by the law - international law and its customary counterpart, in this case - is therefore permitted. As argued by Schmitt, the legal framework surrounding the resort to force is evidently prohibitive in nature in that it forbids the use of force. For this reason, it is straightforward to distinguish between the use of armed force, which is prohibited, and other forms of coercion that are not prohibited under Article 2(4) of the United Nations Charter. Hence, actions conducted through cyberspace that entail propaganda, espionage, or forms of economic coercion, to name a few, would not be regarded as uses of force since they are not prohibited under Article 2(4) of the Charter and may breach other principles of international law, but not the prohibition on the resort to force.

The last two criteria are military character and state involvement, and as mentioned before, they were not included in the original list of factors created by Michael N. Schmitt in 1999. With regard to the military character of a cyber operation, if a cyber operation is connected directly or indirectly to other military operations or is part of a military operation, it is more likely that it will be regarded as a use of force. Moreover, the fact that the target of a cyber operation is a military cyber infrastructure rises the possibility of it being regarded as a use of force as well. As for the degree of State involvement, the stronger the connection between a State and the cyber operation in question, the higher are the chances that it will be regarded as a use of force by other States.

To sum up the findings of the analysis on the set of criteria explained above, a cyber operation amounting to armed force is distinguished from other cyber operations in that it causes a certain level of harm - injury or death to persons, damage or destruction of objects; its consequences manifest more imminently than in other forms of coercion; also, the consequences of the malicious cyber operation manifest in a more direct way, that is to say, there is a close nexus between the initial cyber operation and the harmful consequences; a cyber operation amounting to a use of force is more invasive than a cyber operation used for exploitation purposes or cyber espionage, for instance, in that it targets specific IT systems fundamental for national interests and security and does not limit itself to the stealing of data; it is easier to account for its consequences because they are more tangible - there is a number

of casualties, of loss of property, of systems that were corrupted, etc.; the consequences of the action are those that the international community is seeking to avoid by adopting the legal framework on the prohibition of the use of force; there is connection in between the cyber operation and other military activities or the cyber operation is part of a broader military operation; the degree of State involvement is sufficient for other States to attribute the action to the attacker State and condemn it as a use of force.

As stated above, the criteria do not come without flaws and there are surely many points that have to be rethought and better discussed, but it is noticeable that they furnish good guidelines in the categorization of a cyber operation not causing direct injury or death to persons, and/or damage or destruction of property within the existing legal framework on the prohibition of the use of force. Certainly, the criteria have to be understood as operating in concert and the legal analysis of the consequences of a cyber operation has to include if not all of the above, at least the majority of such factors in order to wisely classify a cyber operation as a use of force. Last but not least, it is important to bear in mind that the standard of actions amounting to a 'use of force' and the standard of actions amounting to 'armed attack' serve different legal purposes, although related. As explained in Chapter 1, all armed attacks are uses of force, but not all uses of force are armed attacks. A cyber operation amounting to 'use of force' does not trigger the right of self-defence, while a cyber operation reaching the threshold of 'armed attack' triggers the applicability of the right of self-defence. States victim to a cyber operation amounting to a use of force will have to respond to it by measures other than the use of force in self-defence. When a cyber operation amounts to 'armed attack' as intended by Article 51 of the United Nations Charter will be a matter of discussion in the following paragraph.

Although the consequence-based approach better fits the needs of the cyber era in the context of the use of force paradigm, the author of this dissertation would recommend to take into consideration also the instrument-based approach and to use the two approaches in concert, in that also the latter furnishes some useful elements of distinction in between what should be considered a use of force and what should not. One approach, in fact, does not necessarily exclude the other. In Chapter 1, the categorization of cyber means has revealed that there are certain cyber tools purposely designed to cause, at different degrees, harmful consequences. Since the instrument-based approach alone is thought to be inaccurate by a

large share of scholars and by the present author herself, the analysis of the instrument, together with the analysis of the consequences it is designed to manifest, could lead to a more accurate and smooth evaluation of cyber operations in the context of the use of force legal regime. In the instrument-based approach there is inherently a certain level of analysis of the consequences it can produce as well, in that the reason of their limitation in usage is that of avoiding their deleterious consequences. What is needed, in fact, is a shift of cognitive approach for which weapons are not characterized by their physical characteristics or by the mechanism through which they cause death or destruction, as it happened traditionally and at the time of the drafting of the UN Charter, but specifically by the death and/or destruction they cause, that is to say, by their effects. This process has already been introduced by Brownlie with the identification of chemical and biological weapons as armed force in 1961 and has been accepted by the international community. To quote Marco Roscini, "it is the instrument used that defines armed force, but the instrument is identified by its (violent) consequences."[147] The two approaches appear to be more linked than most of the literature consulted seems to affirm, even though there is broad agreement over the fact that cyber means, such as viruses, worms, and 'botnets' for instance, can be regarded as weapons. Having said that, it is fundamental to bear in mind that, although a cyber operation is carried out through a cyber weapon with a destructive payload, and thus designed to cause a certain degree of harm, the consequences of such operation have to be severe enough in the context of the reasoning on the use of force paradigm explained both in Chapter 1 and in the present Chapter to be considered as a breach of such paradigm. A cyber operation causing minimal damage, as the destruction of a single computer unit or server may be, although carried out through a cyber weapon, would not be regarded as a use of force. Whether or not a cyber operation reaches the use of force threshold depends on the circumstances discussed above and, since there is no univocal answer to the question proposed, nor a precise demarcation line that clearly indicates where to locate a use of force carried out within the cyber domain in the 'spectrum of consequentiality', the most suitable option is that of a case by case assessment.

On a last stance, there is an ongoing debate over the qualification of data as physical objects, and over the categorization of damage or destruction of such data alone as actions

[147] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 50.

amounting to a use of force, absent of physical damage or incapacitation of infrastructure. According to Michael N. Schmitt, the damage to or destruction of data alone does not rise to the level of a use of force, except in the case of the destruction of data that is specifically designed to be convertible in physical objects.[148] Future State practice and international jurisprudence will surely contribute in the clarification of this topic of discussion.

1.2.1 The disruption of 'national critical infrastructures'

The findings of the analysis above have led to the conclusion that cyber attacks that cause or that will probably cause physical damage or destruction of objects and/or injury or death of persons can be compared to kinetic attacks and, from a legal standpoint can be dealt with in the same way. The use of force legal regime would thus be applicable to cyber operations by relying on the 'physical consequences equation' in between cyber attacks and kinetic attacks. Due to the constant increase in reliance on computer networks and computer systems both by the civil society and by national authorities, some scholars - as Schmitt, Melzer and Roscini - find the 'physical consequences equation' as being too narrow. Their argument is based on the instance that cyber operations causing severe disruption, instead of physical destruction, could also amount to a use of force in the sense of Article 2(4) of the United Nations Charter, depending on the severity of the consequences they manifest. Furthermore, Roscini and Melzer argue that, in absence of direct consequences entailing injury and/or death of persons or damage and/or destruction of objects, more attention should be addressed to cyber operations causing the disruption of the so-called 'national critical infrastructures', in the cases in which their disablement - or the incapacitation of some of the IT systems they entail - endangers national security.

The protection of NCIs has become a pressing issue both for Sovereign States and for regional and international organizations. The topic is included in the national security strategies of a good number of States, as well as in debates at international level regarding cyber security. This is evidence of the importance that States confer to their NCIs, and

---

[148] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict", in Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 55.

supports the argument for which severe disruption of NCIs could be considered as a use of force as well. Nevertheless, also in this case, there is no general agreement in what national critical infrastructures consist of. States have separately included a definition of NCIs in their national security strategies or glossaries of military terminology. Although they may engage in different political doctrines and beliefs, coming from their own peculiarities and cultural traits, a general common definition of national critical infrastructures could be inferred. The European Union, in Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure, defined critical infrastructure as:

> "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, 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."[149]

The official definition of NCIs given by the UK government, at the time of writing, is:

> "Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or b) [s]ignificant impact on national security, national defence, or the functioning of the state."[150]

The United Kingdom recognizes thirteen sectors as part of their national critical infrastructures, namely civil nuclear, communications, space, emergency services, defence, chemicals, finance, transport and water, government, food, health, and energy.[151]

The Russian Federation, instead of referring to national critical infrastructures, refers to 'vital infrastructure' in the context of cyber security, and defines it as:

> "[a] State's facilities, systems and institutions, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, energy supply, credit and finance, communications, State administrative bodies, the defence system, law-enforcement agencies, strategic information resources, scientific establishments and scientific and technological

---

[149] European Union, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection*. 8 December 2008, Article 2(a).

[150] Center for the Protection of National Infrastructure, *Critical National Infrastructure*, available at; https://www.cpni.gov.uk/critical-national-infrastructure-0, accessed 14 May 2020.

[151] Cabinet Office, *Public Summary of Sector Security and Resilience Plans 2017*, London (December 2017): p. 5.

developments, installations that pose heightened technological and environmental risks, and bodies for eliminating the consequences of natural disasters or other emergency situations)."[152]

Similarly to the European Union, for National Critical Infrastructures the United States intends: "[s]ystems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters [...]."[153] The United States Cybersecurity and Infrastructure Security Agency (CISA) identifies 16 sectors forming part of the US national critical infrastructure, namely: chemicals; communications; commercial facilities; critical manufacturing; dams; defense industrial base sector; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; water and wastewater systems.[154]

Lastly, the Shanghai Cooperation Organization, for NCIs refers to "[...] public facilities, systems and institutions attacks on which may cause consequences directly affecting national security, including that of the individual, society and state."[155]

Notwithstanding a few differences in these definitions, it is evident that many States and regional organizations, despite their different political views and doctrines, identify 'national critical infrastructures' as those sectors and services that are vital for national security, including sectors regarding the delivery of basic services that are essential for the lives of citizens - as the sectors that concern supply of food and water. Furthermore, sectors such as government, communications, finance, energy, transportation and emergency services are frequently classified as national critical infrastructures. The definitions given above also mention that not only the destruction of such assets, facilities, systems, networks or processes, but also the disruption of such infrastructures could endanger national security. The severity of the disruption is an essential factor for the classification of the cyber operation causing the disruption itself to be classified as a use of force under Article 2(4) of

---

[152] UN Secretary-General, Australia, Belarus, Brunei Darussalam, Cuba, Oman, Qatar, Russian Federation, Saudi Arabia, United Kingdom, United States, *Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General*, UN Doc A/54/213, 10 August 1999, p. 10.

[153] Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Directors of the Joint Staff Directories, *Joint Terminology for Cyberspace Operations*, November 2011, para 9, p. 5.

[154] Cybersecurity and Infrastructure Security Agency, *Critical Infrastructure Sectors*, last revisited on 24 March 2020, accessed 14 May 2020, available at: https://www.cisa.gov/critical-infrastructure-sectors

[155] Nils Melzer, *Cyberwarfare and International Law*, p. 15.

the UN Charter. In agreement with Marco Roscini, considering if the target of a cyber operation is part of what we have discovered to be considered 'national critical infrastructure' can be of great help in the classification of the cyber operation as a use of force, if not for inclusion, at least for exclusion. Furthermore, the definitions given above show that cyber operations severely disrupting NCIs are likely to be considered as a 'use of force', of course depending on the degree of severity of the consequences they manifest, since they may halt the delivery of essential services to entire societies.

Ultimately, we have come to the conclusion that the three approaches explained in the paragraph above, if considered in conjunction, can lead to an accurate analysis of cyber operations, and that the application of one approach does not necessarily exclude the others. However, it is important to notice that, if only one of the three approaches were to be used, the effect-based approach would be the one providing a more accurate and solid evaluation of the cyber operation in question and would better fit into the use of force paradigm.

As experience with cyber operations and cyber attacks increases, due to their more and more frequent use, the possibility for significant economic consequences or severe disruption of vital functions for the society to be classified as a use of force should not be excluded, even in lack of injury and/or death of persons, or damage or destruction of physical objects. It is important to consider, in fact, that due to the high reliance of our society on IT systems, "cyber technologies have enabled states to produce results analogous to those of kinetic weapons but without the need of physical damage."[156] The evolution of state practice and of the reasoning of international jurisprudence will reveal whether the interpretation of Article 2(4) of the UN Charter will be enlarged to include also the (severe) disruption of NCIs as uses of force, or even as armed attacks under Article 51 of the same Charter.

1.3 Cyber Operations as Threat of force

Article 2(4) of the UN Charter, as explained in Chapter 1, apart from prohibiting the resort to the use of force, prohibits also the threat of force. A threat of force is considered to be unlawful when the use of force threatened itself, if implemented, would be unlawful.

[156] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 61.

Certainly, in order for a threat of force to be a breach of Article 2(4), it must not be an action carried out for self-defence purposes and it must not have been authorized by the United Nations Security Council under Chapter VII of the UN Charter. Accordingly, in the *Tallinn Manual 2.0*, the NATO CCD COE International Group of Experts applies the rule to the cyber domain by stating in its Rule 70 that "[a] cyber operation or threatened cyber operation constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force." Rule 70 envisages two different situations that may take place in the cyber realm: in the first case, a cyber operation is used to communicate a threat of force, be it kinetic or cyber in nature; in the second case, the cyber operation threatened corresponds to the cyber operation that, if carried out, would constitute a use of force, and it can be notified through means that are either cyber or not - e.g., through a cyber operation notifying the possible implementation of a cyber operation that constitutes a threat of force, or through a public statement. It is important to bear in mind that, in both cases, in order to fall under the scope of the use of force paradigm, the threat of force has to be clearly identifiable and it has to be communicated to the threatened State in order to be considered a coercive action. The threat can be communicated both implicitly or explicitly, but to be considered as such, it must have a communicative nature, that is to say, it must be clear that it addresses a particular State, and such target State must have understood that it is the target of a threat of force. An example of an implicit threat of force in the cyber realm could be a cyber warfare simulation or the simulation of other cyber military exercises in a context of tension between States.[157]

As for the acquisition of nuclear armaments, also the mere acquisition of cyber capabilities should not be considered a threat of force, unless the State acquiring such capabilities communicates its intention to use them against another State, present a conditional basis or not.[158] Therefore, in the latter case, the acquisition of cyber capabilities with the intention to use them against another State would be a threat of force breaching Article 2(4) of the UN Charter. However, as Roscini explains, secret cyber warfare exercises should not be considered a threat of force, because they would lack one fundamental element for a threat of force to be coercive, that is, the target of the threat itself.[159]

---

[157] ibid., p. 68.

[158] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 338.

[159] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 68.

Finally, as the actions amounting to traditional uses of force are applicable, *mutatis mutandis*, to those that amount to threats of force, the conclusions reached with regard to the illegality of certain cyber operations and their classification as uses of force argued in the paragraphs above also apply to those actions that amount to threats of force.

2. Cyber attacks as 'armed attacks'

The findings of the analysis regarding what constitutes a use of force reaching the threshold of 'armed attack' discussed in Chapter 1 have lead us to different conclusions. In the first place, all armed attacks are uses of force, but not all uses of force are armed attacks. For a use of force to be considered as an 'armed attack', thus triggering the right of self-defence embedded in Article 51 of the UN Charter and its customary international law counterpart, the action has to be 'a grave form' of use of force, causing severe injury and death of persons and/or severe damage and destruction of property.

In the second place, instead of facing the interpretative conundrum concerning the meaning of 'armed attack' from an act-based approach, that identifies an 'armed attack' based on the fact that the action in question has been carried out with the use of a conventional weapon, the effect-based approach moves the spotlight to the consequences caused by the coercive action. If such consequences, measured through the 'scale and effects' criterion, are severe enough to reach the threshold of armed attack explained above, the action will be considered as such in spite of the tools used for its execution. As a consequence, an armed attack need not be carried out through the use of a conventional weapon. Therefore, attacks carried out through the use of cyber weapons would also fall into this category, given that their consequences are sufficiently grave to reach the 'armed attack' threshold, that is, given that they cause considerable loss of lives and extensive destruction of property. If cyber operations were to be evaluated under the 'scale and effects' criterion, second-order effects could reach the required level of harm.

Finally, an armed attack, to be considered as such, need not be conducted necessarily by the regular army of a State. Attacks carried out by mercenaries, irregular forces or groups can be attributable to a State depending on its degree of involvement. Furthermore, after the 9/11

attacks against the United States, the notion of armed attack has expanded to englobe also actions carried out by terrorist groups, absent of State involvement. Although the United Nations Security Council did not explicitly recognize these terrorist attacks as armed attacks triggering the right of self-defence, it allowed the resort to force in self-defence in Resolutions 1368 and 1373.

Cyber attacks that cause substantial harm or material destruction can be considered as armed attacks for the purposes of the right of self-defence. As affirmed in Chapter 1, for cyber attack we mean: those cyber operations whose aims are altering, deleting, corrupting, or denying access to computer data or software, with the purposes of 1) deception or propaganda; and/or 2) partially or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure; 3) producing physical damage extrinsic to the computer, computer system or network.[160] The nature of the payload they carry is destructive, in contrast with the one carried by cyber operations for exploitation purposes for instance, which acquire information non-destructively. Cyber attacks are conducted via cyber weapons, that are codes designed to damage a computer or computer system or network usually pertaining to national critical infrastructures, so to facilitate the partial or total interruption or even alteration of their operations. Cyber weapons can be defined also as malicious codes programmed with the purpose of causing - directly or indirectly- physical damage to property or people.

To sum up, a cyber attack is conducted through the use of a cyber weapon, that carries a destructive code with offensive capability, and that was designed with the intent of damaging and/or destructing objects or even injuring and/or causing death of persons. A cyber attack as described, given that it causes the sufficient amount of harm for the 'scale and effects' criterion, fits into the definition of armed attack given above.

The effects of cyber attacks can be classified in three categories: 1) first-order effects are those affecting the targeted IT system; 2) second-order effects are those that manifest outside the targeted IT system, but that are strictly connected to it; 3) third-order effects are long-term effects caused by the sum of the first-order and second-order effects, and are identifiable in societal, political, and strategic changes of and within the victim State. An example of a cyber attack is that of an operation directed against an air traffic control system,

---

[160] See Chapter 1, p. 61; and Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 17.

that alters the information concerning the position of aircrafts, producing direct effects on the air traffic control system itself since it compromises its functioning. Apart from this first-order effect, which manifests inside the IT environment, the cyber attack in question can have second-order effects, that are outside the IT environment, such as the crash of aircrafts, that result not only in physical damage but also in loss of human lives.[161] Second-order effects may be the intended effects of the initial cyber attack. In such case and depending on the severity of the harm produced, a cyber attack could rise to the level of 'armed attack'.

Following the reasoning of the paragraph above, another question to be answered is whether cyber attacks on national critical infrastructures causing their severe disruption, but absent of physical damage of property or loss of human lives, could be considered armed attacks triggering the right of self-defence as well. The question arises from the assertion that armed attacks, as Constantinuo opines, can be identified also in actions inflicting "substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure [...] and the use of force which is aimed at a State's main industrial and economic resources and which results in the substantial impairment of its economy."[162] Constantinuo and Roscini, together with other scholars such as Melzer, argue that not only the destruction of physical property or the harm to persons, but also the severe disruption of certain critical infrastructure of a State can be considered an 'armed attack', as the quote above demonstrates. Constantinuo, in fact, considers also the disruption of the economic and industrial infrastructures of a State as consequences of an operation that would reach the level of 'armed attack'. Obviously, the cyber attack under evaluation, independently from its target, would have to fit into the 'scale and effects' criterion explained above. An example of a cyber attack identifiable into the notion of armed attack could be one that disables the computer-controlled life-support systems that could eventually results in loss of human lives. However, taking into account cyber attacks that affect the economic resources of a State stretches significantly the meaning of 'armed attack', allowing self-defence for a broader category of actions for which it was not originally envisaged. In fact, as discussed in Chapter 1, economic coercion was purposely left out of the definition of 'use of force' and consequently can never

---

[161] Nicholas Tsagourias, "*Cyber attacks, self-defence and the problem of attribution*," J*ournal of Conflict & Security Law* Vol. 17, No. 2 (2012): p. 229.

[162] Avra Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter*, (Athens: Sakkoulas, 2000), pp. 63-64.

be considered as an armed attack for self-defence purposes. In the cyber realm, the effects of cyber operations targeting the economy of a State would manifest long after the operation has finished. If this situation were to be considered as an armed attack, it would raise questions regarding the immediacy of the response, or even of the necessity of the forceful response. Nils Melzer supports the argument of including the severe disruption of national critical infrastructures as effects of cyber attacks that would qualify as armed attacks, and the opinion of many States seems to tend to this position. As noted by Roscini, "[i]t is noteworthy that the United States reserves the right to use 'all necessary means' against 'hostile acts' including 'significant cyber attacks' directed not only against the US government or military but also the economy."[163] If this position was to be adopted, a cyber attack against the financial system of a State that causes its severe economic instability or that causes the inability of such State to perform its vital tasks, such as national defence, would be considered an armed attack. The latter example fits more easily into the notion of armed attack, while the former would expand substantially its meaning. As argued in the paragraphs above, however, technological advances have enabled States to inflict deleterious consequences upon the target State without necessarily causing physical destruction or loss of human lives. Moreover, it is important to keep in mind that, even if such cases were included into the notion of 'armed attack', it would not automatically mean that the victim State is entitled to use force against the perpetrator of the attack, because the victim State would have to comply with the principles of necessity and proportionality. Indeed, when measures other than uses of force represent viable options for stopping or repealing an armed attack - such as passive cyber defence or even cyber operations below the level of use of force -, a use of force in self-defence would be neither necessary nor proportionate. The NATO CCD COE International Group of Experts expressed their inability to agree on a joint position on the matter in the *Tallinn Manual 2.0*. According to their discussion, some of the Experts regarded the harm to persons and the destruction of objects as *conditio sine qua non* for the classification of a coercive action as an armed attack; others, considering the extent of the resulting effects of a cyber attack rather than their nature - harmful or destructive -, endorsed the argument for which the disruption of the functioning of a State, as well as long-lasting and severe consequences to its stability, were sufficient to satisfy the armed attack

[163] Marco Roscini, Cyber Operations and the Use of Force in International Law, p. 74.

criterion.[164] Unfortunately, agreement has not been reached on the matter. State practice will tell.

There is debate as to whether the victim State may respond by using force in self-defence to a series of cyber attacks that, taken alone, would not amount to armed attacks but that, if taken together, could reach the severity necessary to amount to armed attack. If such 'low intensity' cyber attacks were to be taken alone instead of cumulatively, they would not amount to armed attack because their consequences would be low intensity as well. In this case, the victim State would have to respond through non-forcible measures. However, if the effects of such 'low intensity' cyber attacks were to be considered as aggregated, they could be overall sufficient to reach the threshold of armed attack. As Tsagourias explains, "frequent - albeit mildly disruptive- attacks on a State's financial system may cause limited damage; but the cumulative effects may be substantial if overall trust in the system is destroyed, which may have been the aim of the individual attacks."[165] He argues that it is probably in these cases that minor cyber attacks would rise to the threshold of armed attack for the purpose of Article 51 of the UN Charter. This may be the key to solve the debate regarding the inclusion of cyber operations that severely disrupt the functionality of national critical infrastructures - such as the economy and industry sectors - but that do not cause material damage or loss of life into the notion of armed attack for self-defence purposes. In fact, only coordinated cyber attacks that severely disrupt a good number of national critical infrastructures of a highly IT-reliant State for an extended period of time would probably meet the 'scale and effects' criterion so to amount to an armed attack.[166] This view is supported by the NATO CCD COE International Group of Experts, that agreed that the determinative factor as to whether a series of cyber incidents taken together can be considered as armed attack is firstly whether they are related, and secondly whether they were carried out by the same originator or originators acting in concert. If they above criteria are met, the 'low intensity' cyber attacks could be considered as a 'composite armed attack'.[167]

---

[164] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, pp. 342-343.

[165] Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," p. 233.

[166] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 75.

[167] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 342.

On a last stance, there is still no agreement regarding the question of intent, that is, as to whether the (aggressive) intent behind a cyber operation is a determinative factor for it to be considered as a cyber attack reaching the threshold of armed attack. In Melzer's opinion, the distinctive element between a 'lesser grave' use of force and a 'most grave' use of force, apart from the scale and effects of the operation, is the intent of the attacker to violate "another state's sphere of influence."[168] In the cyber domain, the aggressive intent can be highlighted by the persistence of the operation, by the sophistication of the methods used, and by the nature of the target - as national critical infrastructures.[169] If Melzer's point of view were to be adopted, it would avoid the unintended spread of malware meeting the scale and effects criterion from being considered as an armed attack for self-defence purposes. The NATO CCD COE Group of Experts was divided over the matter. The majority of them took the position that intention is irrelevant when determining if a cyber operation is an armed attack; in their view, the 'scale and effect' criterion is the most effective when making such determination. A few of them, instead, would not have classified a cyber operation absent of aggressive intent - e.g., cyber espionage - as armed attack, since its effects are unintended, despite the fact that they meet the 'scale and effects' criterion. Intention is surely important when classifying a cyber operation as cyber attack, since its payload is intentionally destructive. However, due to the fact that cyber incidents are not so remote from happening, finding common grounds on the classification of a non-destructive cyber operation accidentally causing sufficient harm or destruction to meet the scale and effects criterion as armed attack is becoming urgent. Again, State practice will tell. In any case, the response to the unintended armed attack would have to satisfy the principle of necessity and proportionality, that will be better discussed in the following sections.

2.1 Cyber attacks and self-defence

As we have seen, the classification of a cyber attack as armed attack for the purpose of self-defence is not so straightforward. Certainly, cyber attacks that cause considerable loss

---

[168] Nils Melzer, *Cyberwarfare and International Law*, p. 16.

[169] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 77.

of lives and extensive destruction of property are classified as armed attacks for the purposes of Article 51 of the UN Charter. For what concerns the severe disruption, instead of destruction, of important elements of a State - such as NCIs-, agreement has not been reached yet.

The overall position of the NATO CCD COE International Group of Experts with regard to the application of the right of self-defence to the cyber context is expressed in Rule 71 of the *Tallinn Manual 2.0*, that states:

> "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[170]

The main criterion in the determination as to whether a cyber operations reaches the level of armed attack so far is that of the 'scale and effects'. The seriousness of the attack, as explained in the sections above, is measured by its degree of injury, fatality and damage to persons or physical objects. However, many cyber operations are likely to severely affect the victim State without causing any physical deleterious consequences.

The application of Article 51 of the UN Charter to the cyber context is complicated not only because of the difficulty of classifying a cyber operation as an armed attack itself, but also because cyber attacks rarely come as a single cyber action. Cyber attacks are often 'multi-layered', in the sense that a single cyber attack may be composed of different cyber actions. Therefore, it is important to determine which cyber action constitutes the armed attack triggering the forceful response. For a cyber attack to be executed, there may be the need of a cyber action that maliciously infiltrates the system, and of another cyber action that executes the payload and produces the harmful effects. These cyber actions could take place in different lapses of time, and their effects could manifest in a distant time from the initiation of the attack. Therefore, does the cyber attack begin with the cyber action that infiltrates the targeted system or does it begin when it executes its payload, or even when its effects manifest? On the one side, if a cyber attack is intended as the sum of the cyber actions needed to execute it and manifest its intended effects, the cyber attack would begin from the moment it infiltrates the targeted system, and therefore it would trigger the right of self-defence from that moment. Concerns arise as to whether the initial infiltration of a system can help identify the intensity of the cyber attack that would follow, and as to the applicability of the principles

[170] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 346.

of necessity and proportionality to the action in self-defence to repeal the attack that has initiated. For this matter, it may be useful to look into Yoram Dinstein's notion of 'interceptive' self-defence. Dinstein identifies interceptive self-defence as a "reaction to an event that has already begun to happen (even if it has not yet fully developed in its consequences)."[171] In his view, a self-defensive action can begin when the armed attack has actually began, even though it has not reached its target yet. The beginning of an attack is measured from the "moment of irrevocable commitment to the attack,"[172] before the first shot is fired. Interceptive self-defence could be useful in assessments of the lawfulness of self-defence responses against traditional armed attacks, since it can be placed in between the notions of traditional self-defence and anticipatory self-defence. However, due to the speed at which a cyber attack can be launched - in a matter of seconds, with the click of a mouse -, a reasoning on interceptive self-defence may not be that helpful.

On the other side, if the cyber attack is intended as such from the moment it manifests its effects, the attack would start to exist when its destructive effects manifest, regardless of when the targeted system had been infiltrated or of when the payload had been executed.[173]

Furthermore, cyber attacks often do not come by themselves. An initial cyber operation that does not reach the threshold of armed attack may be preparatory for a second cyber operation reaching such threshold, or for a conventional armed attack. Should the initial cyber operation that enables the kinetic or cyber armed attack be considered as the initial act of the armed attack itself or should it be considered as a separate operation? When a cyber attack is launched in conjunction with a traditional armed attack, the concept of interceptive self-defence may prove to be more useful. On this regard, Dinniss offers a very good example: think of the 2007 Israeli intrusion into the Syrian air defence radar system that preceded the Israeli airstrike against a suspected Syrian nuclear reactor. In *Operation Orchard*, if the Israeli intrusion had been detected, would this have been sufficient to trigger the right of self-defence? Would Syria have been in the position of having to wait for its radar system to be actually manipulated to facilitate the airstrike to engage in a self-defensive action to repel the upcoming attack? In Schmitt's point of view, reported by Dinniss, the determinative element

---

[171] Geoffrey S. DeWeese, "Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence", p. 84.

[172] Heather Harrison Dinniss, "*The Status and Use of Computer Network Attacks in International Humanitarian Law,"* (PhD diss., London School of Economics and Political Science, 2008), p. 83.

[173] Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," p. 232.

as to whether a self-defensive action can be undertaken is whether the action detected is an action merely preparatory or whether it is "an irreversible step in the final chain of events."[174] If the latter option is true, self-defence would be in order.

Another problem surrounding the applicability of Article 51 of the UN Charter to the cyber context is that it is difficult to attribute a cyber attack to its original perpetrator. Consequently, tracing a cyber attack may take a long time, arising questions over the necessity of the use of armed force to repel the cyber attack in question. Additionally, the principle of proportionality, when applied to cyber attacks, is also questioned. Is it proportionate to resort to armed force in self-defence to respond to a cyber attack? The following sections will attempt to answer these questions.

2.1.1 Necessity and proportionality

When a State lawfully resorts to armed force pursuant to Article 51 of the UN Charter, it must comply with the principles of necessity and proportionality. Necessity and proportionality are not included in the provision regarding the lawful resort to armed force in self-defence, but have become part of its customary international law counterpart, as stated in Chapter 1. For the principle of necessity, a victim State's resort to armed force in self-defence is lawful only when it is used as last resort to end the armed attack, that is to say, when non-forcible measures would not be enough to end the coercive action. The use of armed force is, therefore, necessary for a State to defend itself. The principle of necessity is judged by the victim State and it is, thus, a subjective criterion.

For the principle of proportionality, the necessary use of armed force has to be proportionate to the need of repealing an armed attack, that is to say, it must be proportionate to the end of the right of self-defence itself. Both the principles apply to self-defence in the cyber domain as well. Uses of armed force in self-defence also have to comply with the requirements of imminence - of the attack for the purpose of anticipatory self-defence -, and immediacy - of the response after an armed attack has occurred.

---

[174] ibid., p. 84.

Rule 72 of the *Tallinn Manual 2.0* applies the principles of necessity and proportionality as follows: "A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate."[175]

In the cyber context, a victim State may resort to passive or active cyber defence in response to a cyber armed attack. Passive cyber defence, as explained in Chapter 1, are actions taken to defend the networks of a State and can consist in the use of prevention devices and/or intrusion detection devices, for instance. In case passive cyber defence, like firewalls, are sufficient to thwart a cyber armed attack, forceful measures - cyber or kinetic in nature - would be unlawful. Active cyber defence, instead, are attacks in response to previous cyber attacks. They can be actions below the threshold of force or actions reaching the threshold of use of force. If active cyber defence below the level of force are sufficient to repel an ongoing attack or to deter it, a forceful cyber - or kinetic - response would not be necessary and it would thus be illegal. Certainly, and as expressed by the principle of necessity itself, if cyber or kinetic operations short of armed attack fail to thwart an armed attack and prevent future ones, the use of both cyber and kinetic armed force is allowed under the right of self-defence.

The principle of proportionality applied to *jus ad bellum* concerns how much force - kinetic or cyber - is needed to actually repel or halt an armed attack, in case the use of force is necessary. This should not be interpreted as an obligation to respond in-kind or to use force of the same nature as that of the armed attack received, or the same amount of force. To repel an attack, less force or more force than that of the armed attack that triggered the right of self-defence may be needed. As for the nature of the force used, a victim State may resort to uses of cyber force to counter a kinetic armed attack and *vice versa*. This is due to the fact that a response to a cyber attack through a cyber use of force may not always be effective or even an option available. The victim State, for instance, may not be equipped with sufficient technology to respond through cyber means. Also, the aggressor State, in spite of being able to carry out a cyber armed attack, could be a low-technology State with no digital infrastructure to target or even a non-state actor, for which kinetic force might be the only option available.[176]

---

[175] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 348.

[176] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 90.

Lastly, the right to lawfully use force in self-defence is subject to the requirement of immediacy, that applies to the cyber context as well. Immediacy is expression of the fact that the aim of self-defence actions is not that of punishing the aggressor, but to repel or to stop the armed attack. What is meant for immediacy is not that the response in self-defence must be instantaneous, as it refers to the period of time after the armed attack within which the victim State's response in self-defence would be reasonable. The requirement is applied with a certain degree of flexibility, especially in the case of cyber attacks. Due to their nature and to the intrinsic characteristics of the cyber domain, the time required to identify the originator of the attack may not be so short. Moreover, the cyber attack might have debilitated the victim State's military networks or systems, making it harder and time consuming to answer in self-defence through cyber means, for instance. For the peculiarities of the cyber realm, however, a victim State should not be deprived of its right of self-defence.

2.2 Anticipatory Self-Defence

The discussion over self-defence in Chapter 1 has shown that there are different interpretations of the phrase 'if an armed attack *occurs*' contained in Article 51 of the UN Charter. The Article surely applies to situations in which an armed attack has already occurred. In the cyber context, it covers cyber armed attacks that have already occurred, or that are in the process of causing destruction and/or death. However, the evolution of the right of self-defence as customary international law has demonstrated that there is the possibility of taking actions in self-defence in anticipation of an armed attack -be it cyber or kinetic-, as long as there is sufficient evidence to prove that the armed attack in question is imminent. The requirement of imminence has been incorporated in the *Tallinn Manual 2.0* in Rule 73, that states:"The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to the requirement of immediacy."[177]

Dinniss explains that there are two situations in which anticipatory self-defence can be applied to the cyber domain. Firstly, it can be applied to a situation in which a cyber attack is

[177] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 350.

expression of an imminent threat of a traditional armed attack. Secondly, it can be applied to a situation in which electronic activity shows that a cyber armed attack is imminent.

In the first case, that is to say, when a cyber attack is used as preparatory for a conventional armed attack, the assessment of the target of the traditional attack will be of great relevance for the purpose of anticipatory self-defence. If the preparatory cyber attack targets NCIs, such as early warning systems, or military communications, or emergency response systems, it will be more likely that the victim State will consider the upcoming traditional attack as imminent, and therefore that it would act in anticipatory self-defence. Clearly, anticipatory self-defence actions will have to comply with the customary international law principles of necessity and proportionality explained in the sections above. Israel's Operation Orchard is an example that well fits this statement. If Syria had detected the disablement of its air defence radars before the airstrike against its nuclear facility, it would have been entitled to act in anticipatory self-defence. On the contrary, the DDoS against Estonia in 2007, although sustained, were directed against Estonia's banking websites, together with websites belonging to the media and to the government, and for such reason they were not considered to be the prelude to a conventional armed attack.[178]

In the second case, a cyber attack is preparatory for another cyber attack possibly reaching the threshold of armed attack. In this case, the lawfulness of a response in anticipatory self-defence is harder to assess. The preparatory cyber attack can be conducted through the use of malwares such as viruses, worms or Trojan horses, for instance. These malwares could be installed into the targeted computer system in order to cause a malfunction, disable virus protection, corrupt data, or collect passwords and access codes so to allow the perpetrator of the attack to gain access to the targeted system at a later time. Common to these types of malware is the fact that they are able to install a backdoor payload into the targeted system, that also allows the attacker to access the system at a later point in time.[179] Although the establishment of a backdoor payload is indicative of the perpetrator's intention to re-access the targeted system, what remains uncovered is the purpose for its infiltration at a later date. In this case, the victim State, after having detected that its computer systems have been infiltrated and compromised with a malware, would not have sufficient evidence as to

---

[178] Heather Harrison Dinniss, "The Status and Use of Computer Network Attacks in International Humanitarian Law," p. 91.

[179] ibid., p. 92.

whether a cyber armed attack will take place, nor of its intensity and magnitude. As Roscini points out, what is to be taken into account is not the fact that the attacker has gained the capability of conducting a cyber armed attack through the installation of a backdoor or the infiltration of a computer system, but the fact that it has actually decided to conduct the attack, and that the victim state has "no other choice than to act immediately to respond effectively to the (imminent) attack."[180] In absence of evidence, the principles of necessity and proportionality would not be satisfied, and neither would the requirement of imminence. Consequently, acting in anticipatory self-defence would not be in order, while passive or active cyber defences not amounting to a use of force could be sufficient to stop the initial cyber attack.

Anticipatory self-defence - be it through cyber or through kinetic means- against an imminent cyber armed attack alone is considered to be very difficult to invoke. In fact, in lack of evidence concerning the originator of the attack, the nature of the attack itself and its imminence, the necessity and the proportionality of the response in anticipatory self-defence would be impossible to assess.

2.2.1 The challenge of imminence in the cyber realm

The requirement of imminence is particularly interesting when applied to the cyber context. As explained in Chapter 1, a different understanding of the requirement of imminence leads to different understandings of the right of self-defence. In fact, the possibilities of invoking the right of self-defence are positioned along the spectrum of imminence, and range from interceptive self-defence to preventive self-defence.

As for interceptive self-defence, of which Dinstein is the major exponent, actions in self-defence are allowed from the moment that an attack has began, even though it has not hit its target yet. The example given to support this view is that of the Japanese attack against Pearl Harbor, for which, in case the United States had intercepted the Japanese fleet reaching its coasts, it could have acted in interceptive self-defence before the Japanese fleet had actually fired over the naval base of Pearl Harbor. When transposed to the cyber domain,

[180] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 79.

however, interceptive self-defence seems not to be helpful or even possible to invoke, since the speed of cyber operations would prevent them from falling into this category.

Anticipatory self-defence is surely the most accepted and consolidated view on the matter. The interpretation of the requirement of imminence was set out by the U.S. Secretary of State Daniel Webster with regard to the famous *Caroline* incident of 1842, in that he stated that self-defence should concern cases in which its necessity is "instant, overwhelming, leaving no choice of means, and no moment for deliberation."[181] The speed of data transmission in the cyber domain seems to fit very well into the notions of 'instant' and of 'no moment for deliberation' used by Webster. However clear theoretically, the interpretation of the standard of imminence, when put in practice, leads to different views over anticipatory self-defence itself. The narrow interpretation of imminence requires that the armed attack must be about to be launched for the response in self-defence to be lawful, thus imposing a temporal restriction on actions taken in anticipatory self-defence. When transposed to cyberspace, this narrow interpretation of imminence appears untenable, since an aggressor could launch an instantaneous cyber attack within seconds with the click of a mouse.

A better approach to the notion of anticipatory self-defence is that of the so-called 'last feasible window of opportunity', for which a State may act in cyber or kinetic anticipatory self-defence when the aggressor is clearly committed to the launch of an armed attack, and absent of immediate action, the victim State would lose its last opportunity to defend itself against the upcoming, and thus imminent, armed attack.[182] The 'last feasible window of opportunity' may take place immediately before the attack or even long time before the attack takes place. Therefore, if this approach were to be applied, the fundamental question would concern when is the last window of opportunity to act in anticipatory self-defence to thwart or mitigate the forthcoming armed attack. This means that the focus would not be over the temporal proximity of the actual response in anticipatory self-defence to the imminent attack, but instead over "whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts."[183] Theoretically, each different victim state has a different 'last window of opportunity' to take

---

[181] Letter from Daniel Webster to Lord Ashburton (6 August 1842), in Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 350.

[182] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 351.

[183] ibid.

actions to stop or mitigate the forthcoming attack. This depends on the characteristics and capabilities of the victim State. In the words of Michael N. Schmitt,

> "[a] weak state may be justified in acting sooner than a stronger one, when facing an identical threat, simply because it is at greater risk in having to wait. The greater the relative threat, the more likely preemptive actions are to be effective, and, therefore, the greater the justification for acting before the enemy can complete preparations and mount its aggressive attack."[184]

The evaluation of the 'last window of opportunity' has to be made in good faith and with the information available at the time of the evaluation itself. This concept also opens the road for pre-emptive self defence, which interprets the requirement of imminence as being more extensive than that used in the traditional notion of anticipatory self-defence.

When talking about anticipatory or pre-emptive self-defence, one has to distinguish two different situations to assess the requirement of imminence through the 'last window of opportunity standard: 1) a cyber attack constitutes the initial phase of an armed attack -cyber or kinetic in nature-; 2) a cyber attack is preparatory for another cyber or kinetic armed attack. In the first case, the *Tallinn Manual 2.0* uses the example of the insertion of a logic bomb, that would qualify as imminent armed attack only when the specific conditions that lead to its activation are likely to occur.[185] In the second case, instead, the creation of a backdoor by an aggressor without any other indicator of whether an attack will take place, of the time of such attack, of its intensity and magnitude, would not meet the imminence criterion and would not authorize a response in anticipatory self-defence. In other words, acquiring the capability to initiate a cyber or kinetic armed attack at an indeterminate time does not satisfy the requirement of imminence. When the aggressor manifests its intention to use its capability to initiate an armed attack and thus to launch the armed attack in question, the requirement of imminence would be satisfied at the point in which the victim State enters in its 'last feasible window of opportunity' to defend itself.

The NATO CCD COE International Group of Experts agreed that the 'last feasible window of opportunity' criterion, although it better fits the needs of operations conducted through or within cyberspace, is "a rather open standard that is subject to interpretation and therefore prone to abuse."[186] Such standard was judged as not being *lex lata*. Only future state practice

---

[184] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: thoughts on a normative framework," p. 931.

[185] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 352.

[186] ibid., p. 353.

will ease the process of clarification as to where the law stands on this matter. On the one side, States that are frequently the targets of cyber attacks or that engage in aggressive policies are more likely to prefer a more flexible approach to imminence. On the other side, States that are not really engaged into the cyber arena are more likely to prefer the aforementioned narrow interpretation of imminence, since they fear possible abuses of a flexible interpretation of imminence by more powerful or simply more technologically advanced States.

Preventive self-defence, as in conventional international law, is considered unlawful as well when applied to the cyber context. As for nuclear weapons, the mere fact that a State has the capability of launching cyber armed attacks is not in itself sufficient to invoke the right of (preventive) self-defence.

To conclude, the speed, unpredictability and covered nature of the majority of cyber operations and of cyber attacks makes it very difficult for a target State firstly to detect the forthcoming cyber attack, and secondly to promptly act to prevent or repeal the forthcoming or ongoing attack. Not to forget is the fact that certain cyber weapons are inherently designed to produce their harmful effects even weeks or months after the targeted system has been infiltrated, as is the case for time bombs. For such intrinsic characteristics of cyberspace and of cyber operations, it will be extremely difficult for a target State to invoke the right of anticipatory self-defence. What is evident is that so far cyber defense must rely mostly on automated systems for the detection of and protection from cyber attacks.

2.2.2 A hypothetical analysis in practice

Following the reasoning of Geoffrey S. DeWeese in his work *Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence*, let us pretend that cyber defence automated systems belonging to State A detected that its air defence system has been infiltrated by a malicious code. Therefore, State A concludes that its computer system is at risk together with its air defence system. There is evidence that the malicious code originated from State B. Moreover, the two States do not enjoy good interstate relations, that is to say, they are adversaries in the international arena. However, State A does not have

any evidence on how State B is planning to use the malware that it infiltrated in State A's air defence system. How is State A going to assess whether it can invoke the right of anticipatory self-defence? Before invoking self-defence, the first options available to State A are 1) that of reporting the happenings to the United Nations Security Council, or 2) that of confronting State B directly; and 3) that of removing the malicious code through cyber defence operations. It is important to bear in mind that States may resort to the use of armed force in self-defence only as a last resort, when non-forceful measures are not sufficient to stop or prevent the coercive behavior of the attacking State, and until the United Nations Security Council is able to take the necessary measures to restore international peace and security. However, strategically speaking, engaging in such peaceful measures would alert State B that State A has found out about the malicious code and, if the intention of State B were coercive, it would give State B the final push to carry out the armed attack before measures are taken against its coercive behavior. Therefore, the best option State A enjoys at the moment is that of removing the malicious code through cyber defence operations. This, however, could imply several difficulties and could give evidence to State B that State A is acting to remove the malicious code. State B, in this scenario as well, could decide to enact the armed attack -cyber or kinetic in nature-, before its possibilities are ruled out. Since none of the options above would guarantee State A's security, State A may conclude that its only option available is that of using force in self-defence, considering also that the malicious code was infiltrated in one of its national critical infrastructures and that an attack against it could have deleterious consequences. In State A's point of view, force would thus meet the principle of necessity. The following step, when finding out that a forceful response is necessary to repel a forthcoming attack, is the satisfaction of the requirement of imminence. Under the conditions displayed above, State A does not have any further element to determine that State's B armed attack is imminent. Nevertheless, according to the 'last feasible window of opportunity' approach, State A could conclude that it must act quickly to prevent State B's attack, before it loses this last opportunity available. Its resort to force in anticipatory self-defence, or pre-emptive self-defence in this case, might not receive the support of the international community since the legal basis for this kind of action lacks sufficient evidence with regard to the forthcoming armed attack. The armed attack that would follow is a mere supposition of State A, arguably reasonable given that State A and State B do not enjoy good

interstate relations. State A may decide to engage in forceful self-defence actions in any case, given that the assessment of imminence and of necessity rely upon the victim State's perspective. Certainly, the anticipatory response in self-defence need to meet the principle of proportionality as well, for that State A's response in anticipation of the attack would have to be limited to the purpose of preventing State B to actually carry out the armed attack.

There are two possible and more probable outcomes from State A's action in anticipatory self-defence. The first is that it successfully prevents State B from carrying out the armed attack that State B had *actually* planned on conducting. If this were true, State A would have protected its territory from being damaged or destructed and its people from being injured or killed, and the purpose of anticipatory self-defence would have been served. The second outcome is that State B had only infiltrated State A's air defence systems for the stealing of data, for instance, and that it was not planning on attacking State B in the proximate future. If the latter outcome was the one produced, State A would have abused of its right of self-defence, although the initial cyber operation that infiltrated the malicious code was directed against State A's national critical infrastructures.

As this example demonstrates, although the law surrounding the use of armed force in self-defence is applicable to the cyber context, the peculiarities of the cyber realm challenge the notion of anticipatory self-defence in general, and that of imminence in particular. In agreement with the position taken by the NATO CCD COE International Group of Experts, the notion of anticipatory self-defence should not be regarded as *lex lata* when applied to the cyber domain. An extensive interpretation of imminence and the acceptance of anticipatory self-defence against cyber threats could lead to abuses of uses of force, that are contrary with the purposes of the United Nations and of the law surrounding both the prohibition of the use of force and that of the right of self-defence, whose main aim is that of limiting the resort to force itself. In the opinion of the author of this dissertation, non-forcible measures could better fit both the needs of the victim State and the aim of the international community to limit the use of armed force - be it kinetic or cyber. State practice and further academic debate will surely lead to a more comprehensive understanding of the matter.

2.3 Collective Self-Defence

The discussion over collective self-defence of Chapter 1 leads to the following conclusions over the requirements for a lawful exercise of the right of collective self-defence, that are: 1) the occurrence of a use of force that reaches the threshold of an armed attack; 2) the declaration of the victim state that it has suffered an armed attack; 3) the request for assistance by the victim State to foreign States, invoking the right of collective self-defence; 4) the duty to report the intent of acting in collective self-defence under Article 51 to the United Nations Security Council. These parameters were set out by the ICJ in the *Nicaragua* judgment and reflect state practice. Additionally, collective self-defence is subject to the same principles as individual self-defence, namely the necessity, the proportionality, and the immediacy of the response.

The same criteria apply to collective self-defence in cyberspace or against a cyber armed attack. The NATO CCD COE International Group of Experts included the provision in its Rule 74, that states:

> "The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim State and within the scope of the request."

Collective self-defence can be exercised also within military alliances, such as NATO, or regional organizations such as the European Union.

As noted by Roscini, NATO has created the Cyber Defense Management Authority, a Computer Incident Response Capability and the already cited CCD COE. However, it is still not clear if its Article 5 can be invoked also with regard to cyber attacks. The cyber armed attack against a certain member State would have to cause dire consequences so to drive the victim member State to invoke Article 5, consequences so dire to resemble the 9/11 attacks against the United States of America, which has been so far the only occasion in which Article 5 has been invoked.

In 2007, when Estonia was the target of sustained DDoS attacks, consultations among NATO members began with regard to Article 4 of the North Atlantic Treaty, and the Defence Minister of Estonia considered even invoking Article 5. However, in that occasion, the Minister claimed that the position of NATO with regard to considering cyber attacks as military actions was not well rooted, and that for such reason, Article 5 was not to be

understood as covering cyber attacks as well.[187] Nevertheless, cyber security is surely very important for NATO. The behavior of the organization, in fact, shows that it is acquiring cyber capabilities, implementing the research on the field as well as academic publications on the matter, organizing annual forums of discussion of Cyber Conflict-related topics, and conducting cyber defense exercises, apart from the signing of Memoranda of Understanding with its member States.

The European Union has become very engaged in cybersecurity matters as well and has been improving its defence capabilities against cyber attacks. Furthermore, it has clearly stated in the European Commission *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace* of 2013 that a severe cyber incident or cyber attack against a Member State could trigger the applicability of the EU Solidarity Clause, that is to say, of Article 222 of the Treaty for the Functioning of the European Union, for which member States will provide aid and assistance in case a member State is victim of an armed aggression, pursuant to Article 51 of the UN Charter.[188] Furthermore, the EU created a specialized Agency for Network and Information Security (ENISA) in 2004, it has conducted several cyber exercises over the years, and adopted the new Cyber Security Strategy on May 27th, 2020, that contains additional measures for the protection of Critical Infrastructure.

[187] Marco Roscini, *Cyber Operations and the Use of Force in International Law,* p. 94-95.

[188] ibid., p. 97.

Chapter 3
Military cyber operations and the *jus in bello*

The previous Chapter revealed when a cyber operations can be considered use of force under Article 2(4) of the UN Charter, as well as when it reaches the threshold of armed attack under Article 51 of the same Charter. Under the *jus ad bellum*, in fact, the resort to force among States is prohibited, except for the resort to force in self-defence granted by Article 51 of the UN Charter and the use of force authorized by the UN Security Council under Chapter VII of the same Charter. Furthermore, Chapter 2 explored how to lawfully use force in self-defence to repeal an ongoing cyber attack and to what extent it is possible to anticipate an imminent cyber attack. However, the analysis conducted so far has been limited to the regulation of the resort to (cyber) force by States in times of peace. Therefore, in order to complete the analysis it is necessary to examine if cyber operations can be regulated within the existing legal framework of the law of armed conflict, and if so, how it applies to military operations conducted through the cyber domain.

Under international Humanitarian Law, attacks can be conducted lawfully if they respect the provisions included in both the Hague Law and in the Geneva Law. The aim of this Chapter will be, indeed, that of determining when a cyber operation amounts to 'attack' in the sense of International Humanitarian Law, and how such body of laws applies to cyber operations during an armed conflict, that is to say, how it applies to cyber operations employed in the conduct of hostilities. The questions that will be addressed in the development of this Chapter are: is International Humanitarian Law applicable to cyber operations? If so, when does a cyber operation amount to 'attack' and is thus regulated by the prohibitions and restrictions for the conduct of attacks during armed conflicts? Consequently, how should such prohibitions and restrictions be applied to cyber operations?

1. Applicability of the Laws of War to Cyber Operations

Already in 1995, the US Air Force Chief of Staff General Ronald R. Fogleman recognized cyberspace as a warfare domain by stating in his speech to the Armed Forces Communications-Electronics Association that "[...] we're crossing a new frontier. Information has an ascending and transcending influence - for our society and our military forces. As such, I think it is appropriate to call information operations the fifth domain of warfare."[189] General Fogleman was not mistaken, given that in the past two decades cyber operations have been used in the conduct of military operations during armed conflicts. Although only a small number of States have publicly admitted that they have been using cyber operations during armed conflicts, an increasing number of States is investing in the development of military cyber capabilities. Cyber warfare, defined in Chapter 1 as "operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means or methods of warfare in the context of an armed conflict,"[190] is now a reality.

Nowadays, it seems uncontested that International Humanitarian Law applies to cyber operations carried out during an international or non-international armed conflict. The same reasoning made for the applicability of the UN Charter regime to cyber operations can be made for the applicability of LOAC. The fact that the advent of cyber operations could not have been envisaged when the most important instruments of IHL were drafted and adopted should not translate into the impossibility of applying such instruments to cyber operations. In fact, the 2015 Report of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security not only confirmed that international law "is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT

---

[189] United States Department of Defence, *Information Operations: The Fifth Dimension of Warfare. Remarks as delivered by Gen. Ronald R. Fogleman, Air Force chief of staff, to the Armed Forces Communications-Electronics Association, Washington, April 25, 1995*, Defense Issues: Volume 10, Number 47, American Forces Information Service, Washington D.C., 1995.

[190] See Chapter 1, p. 62; and ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Recommitting to the Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, ICRC, 2019, p. 26.

environment,"[191] but also noted "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction."[192] Furthermore, the ICRC strongly affirms that International Humanitarian Law applies to cyber operations in both its position paper submitted in November 2019 to the UN GGE and in several of its annual reports. The ICRC had taken its position already in 2011, when it stated that "the employment of cyber capabilities in armed conflict must comply with all the principles and rules of IHL, as is the case with any other weapon, means or method of warfare, new or old."[193] Notwithstanding the characterization of cyberspace - be it a warfare domain just like land, sea, air and outer space, or a distinct kind of domain since it is man-made - customary International Humanitarian Law rules on the conduct of hostilities are applicable to all means and methods of warfare, regardless of where - that is to say, in which warfare domain- they are employed.[194] In support of what has been said so far, it is important to recall the statement of the ICJ contained in its 1996 *Advisory Opinion* on the legality of Nuclear weapons, in which the Court stated that the principles and rules of International Humanitarian Law apply "to all forms of warfare and to all kinds of weapons."[195] By logic, one can even argue that the aim behind the adoption of IHL treaties is precisely that of regulating both present and *future* conflicts, and consequently future means and methods of warfare. Article 36 of Additional Protocol I to the Four Geneva Conventions, in fact, requires that:

> "[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

As a matter of fact, "if IHL did not apply to future means and methods of warfare, it would not be necessary to review their lawfulness under existing IHL,"[196] as required by Article 36 of AP I. Last but not least, not to forget is the Martens Clause that, as explained in Chapter 1,

---

[191] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General*, A/70/174, 22 July 2015, p. 12.

[192] ibid., p. 13.

[193] ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts*, ICRC Reports, 32nd International Conference of the Red Cross and the Crescent, Geneva (2015), p. 40.

[194] ibid.

[195] ICJ, *Legality of the threat or the use of nuclear weapons, Advisory Opinion, 8 July 1996*, ICJ Reports 226, 1996, para 86.

[196] ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, p. 40.

is included in the Hague Convention IV,[197] the four Geneva Conventions of 1949,[198] and in its Additional Protocol I of 1977,[199] and states:

> "Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience."

Cases that do not fall within the scope of the existing IHL are still subject to customary International Humanitarian Law, and thanks to the Martens Clause, also to the principles of humanity and of public conscience. The NATO CCD COE International Group of Experts agreed unanimously in that "cyber operations executed in the context of an armed conflict are subject to the law of armed conflict,"[200] be the armed conflict international or non-international in character.

Three different scenarios can trigger the application of IHL, both to cyber or kinetic operations, or a combination thereof, namely 1) in case of combat action that follows a formal declaration of war; 2) in case of a pre-existing international or non-international armed conflict; and 3) when - and if - cyber operations amount to 'resort to armed force' or 'armed confrontation' under IHL themselves.

In the first case, a formal declaration of war marks the interruption of the application of the laws of peace, while the laws of war begin to apply. A formal declaration of war can be delivered through cyber or kinetic means and, as in the case of kinetic operations, cyber operations following a formal declaration of war conducted by a party to the conflict against the other will be regulated by LOAC.

In the second case, what brings into application the laws of war is not a formal declaration of war, but the existence of an 'armed conflict'. The Geneva Conventions do not define what an 'armed conflict' is. As explained in Chapter 1, the definition adopted by the ICTY in 1995 in the *Tadić* case is now universally accepted, and it affirms that "an armed conflict exists whether there is a resort to armed force between States or protracted armed violence between

---

[197] Hague Convention IV, Preamble.

[198] Geneva Convention I (GC I), Art. 63; Geneva Convention II (GC II), Art. 62; Geneva Convention III (GC III), Art. 142; Geneva Convention IV (GC IV), Art. 158.

[199] Additional Protocol I, Art. 1(2).

[200] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Rule 80, p. 375.

governmental authorities and organized armed groups or between such groups within a State."[201] Since international and non-international armed conflicts have different requirements to exists, the two types of armed conflicts will be dealt with separately. For an international armed conflict (IAC) to be exist, two requirements must be met: 1) the 'resort to armed force'; 2) armed force has to be used between States. In the cyber context, the NATO CCD COE Group of Experts stated that:

> "[a]n international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, between two or more States."[202]

The rule is derived from Common Article 2(1) of the four Geneva Conventions of 1949, in that it transposes the Article to the cyber context. For a non-international armed conflict (NIAC) to exist, there must be: 1) protracted armed violence; 2) such armed confrontation has to take place between a State and an organized armed group, or between organized armed groups inside the same State. A further requirement for non-international armed conflicts to exist is that hostilities have to be substantial, protracted, and large-scale. With regard to non-international armed conflicts in the cyber context, Rule 83 of the *Tallinn Manual 2.0* affirms that:

> "[a] non-international armed conflict exists wherever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and organized armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must have a minimum degree of organization."[203]

The Rule is self-explicative and does not need further discussion, as it is a general restatement of customary International Humanitarian Law. Given that an IAC or a NIAC exists, IHL would apply to cyber operations if the cyber activities in question have a 'belligerent nexus' with the ongoing armed conflict, that is to say, if they are conducted by a party to the conflict against the opposing party or otherwise be related to the armed conflict, so to qualify as acts of hostilities.[204] In fact, the ICRC states that for an act to have a 'belligerent nexus', it has to be "specifically designed to cause the required threshold of harm

---

[201] Prosecutor v Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Interlocutory Appeal), Case No IT-94-1-AR72 (2 October 1995) 35 ILM 35, para 70.

[202] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Rule 82, p. 379.

[203] ibid., p. 385.

[204] The notion of 'hostilities' indicates the resort to means and methods of injuring the enemy by the parties to the conflict that are not limited to the infliction of death or injury of persons, damage or destruction of objects. The concept of 'hostilities', in fact, is a broader than that of attack, as it includes any act undertaken by a party to the conflict to negatively affect the military operations of the adversary, or even its military capacity.

in support of a party to the conflict and to the detriment of another."[205] This means that cyber operations that are carried out for reasons other than the armed conflict itself and thus, that lack of a 'belligerent nexus', will not be governed by LOAC, even if they are carried out by a party to the conflict against the other or within the territory where the combat takes place. However, it is necessary to point out that applying the laws of war to cyber operations can prove challenging. To name a few problems in this regard, the existence of a cyber operation is often difficult to identify; finding the originator of the cyber operation can be time-consuming and success on the matter is not assured; and it is difficult to identify the intended effects of the operation. Furthermore, in the case of non-international armed conflicts, it will be more challenging to establish the 'belligerent nexus' of cyber operations, since it is often difficult to distinguish between cyber acts of hostilities and cyber crimes.[206]

In the third case, LOAC would apply to cyber operations if and when such operations reach the threshold of international armed conflict or non-international armed conflict *themselves*, regardless of the occurrence of kinetic hostilities.[207] If and when cyber operations alone can give rise to an armed conflict will be discussed in the following section.

1.1 Can Cyber Operations give rise to an armed conflict?

So far, when determining if LOAC applies to cyber operations, we have considered only two scenarios, namely, 1) the applicability of the laws of war to cyber operations carried out after a formal declaration of war; 2) the applicability of IHL to cyber operations carried out during pre-existing international or non-international armed conflicts. Nevertheless, it is interesting to take into account also a third scenario, that is, whether cyber operations *alone* can give rise to an armed conflict and thus trigger the application of IHL.

As argued in Chapter 1, the employment of the term 'armed conflict' instead of that of 'war' in the Geneva Conventions of 1949 enlarged the scope of International Humanitarian Law so to include the resort to armed force between States in lack of a formal declaration of war. The

---

[205] Recommendation V(3), in ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Geneva, 2009 (prepared by Nils Melzer), p 58.

[206] ibid., 148.

[207] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 120.

definition of the term 'armed conflict' given by the ICTY in the *Tadić* case highlights that the fundamental element for an armed conflict to exists is the 'resort to armed force', both in the case of IACs and NIACs. When cyber attacks are carried out together with kinetic attacks, there is broad consensus that they can give rise to an armed conflict and thus trigger the application of IHL.[208] However, the question that needs to be addressed is whether cyber operations *alone* amount to 'resort to armed force' under the *jus in bello*.

The notion of 'armed force' under the *jus ad bellum* has already been discussed both in Chapter 1 and in Chapter 2. The discussion led to the conclusion that cyber operations can amount to 'armed force' under the use of force paradigm depending on the consequences that they manifest - effect-based approach. However, under the *jus in bello*, not all uses of 'armed force' as intended by the *jus ad bellum* give rise to an armed conflict. In fact, in the *Nicaragua* judgement, the ICJ stated that "use of force may in some circumstances raise questions of [IHL],"[209] implicitly saying that not all uses of armed force as intended by the *jus ad bellum* automatically amount to 'resort to armed force' under the *jus in bello*. State practice demonstrates that certain minor uses of force, such as cross-border incidents, have not raised questions of IHL and have been dealt with under the UN Charter regime. The arming and the training of the *contras* in the *Nicaragua* case, although qualifying as use of force under the *jus ad bellum*, did not give rise to an armed conflict, for instance. Accordingly, isolated cyber operations below the threshold of 'resort to armed force' would not give rise to an armed conflict. To give rise to an armed conflict, a cyber operation must be able to injure the enemy. Under the *jus ad bellum*, cyber operations capable of causing or that are likely to cause injury or loss of life and/or damage or destruction of property, together with cyber operations that severely disrupt NCIs are considered grave forms of uses of force reaching the threshold of armed attack, and thus subject to the prohibition of Article 2(4) of the UN Charter and to the right of self-defence under Article 51 of the same Charter. The challenge lies in establishing whether such cyber attacks would suffice to give rise to an armed conflict, and whether there is a threshold of harm required for a cyber operation to amount to 'resort to armed force' under IHL so to trigger the applicability of the laws of war.

---

[208] Eric Pomès, "Technological Innovations and International Humanitarian Law: Challenges and Tensions," *Polish Political Science Yearbook* vol. 46, No. 2 (2017), p. 209. DOI: 10.15804/ppsy2017213

[209] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, Merits, Judgement, 27 June 1986, ICJ Reports 1986 (*'Nicaragua'*), para 216; and Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 128.

The position of the ICRC on that matter is affirmative, as it states that "there would be no reason to treat a cyber operation resulting in the destruction of civilian or military assets or in the death or injury of soldiers or civilians differently from equivalent attacks conducted through more traditional means and methods of warfare."[210] Therefore, when a cyber operation causes death or injury of persons or destruction of assets, it amounts to 'resort to armed force' and can give rise to an armed conflict. However, the ICRC does not mention the case of cyber operations severely disrupting NCIs without concurrent physical damage. In support of the ICRC position, Yoram Dinstein argues that violence - intended as violent consequences- is essential for the characterization of certain actions as hostilities.[211] It can be noted that both Dinstein and the ICRC seem to imply that disruptive cyber operations cannot give rise to an international armed conflict, while destructive cyber operations can. If this view was to be adopted, a cyber operation launched with the aim of neutralizing a State's air defence network that does not resulting in physical damage or injury or death of persons would not initiate an armed conflict, for instance.[212]

Although there is broad agreement that cyber attacks causing injury or loss of life and/or damage or destruction of objects can be regarded as 'resort to armed force', some authors argue that 'armed force' is not a definitive criterion that demonstrates the existence of an armed conflict in that a cyber operation could severely disrupt a State's ability to perform essential tasks, such as defence and national security, without causing physical damage. Nils Melzer is one of the main exponents of this view, and he argues that the existence of an armed conflict does not depend on the 'resort to armed force', but rather on the occurrence of 'belligerent hostilities.'[213] The notion of 'hostilities', in fact, is a broader concept than that of 'armed force' as it indicates the resort to means and methods of injuring the enemy[214] by the parties to the conflict that are not limited to the infliction of death or injury of persons, damage or destruction of objects, but that include any act undertaken by a party to the conflict to negatively affect the military operations of the adversary, or even its military

---

[210] Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations*, p. 71.

[211] Yoram Dinstein, The Conduct of Hostilities under the Law of Armed Conflict, (Cambridge: Cambridge University Press, 2010), p. 1.

[212] Heather Harrison Dinniss, "*The Status and Use of Computer Network Attacks in International Humanitarian Law"*, (PhD diss., London School of Economics and Political Science, 2008), p. 119.

[213] Nils Melzer, *Cyberwarfare and International Law*, p. 24.

[214] The fact that cyber operations are means and methods of warfare and capable of injuring the enemy is undisputed and the applicability of IHL to the cyber context has already been argued in the section above.

capacity.[215] The NATO CCD International Group of Experts does not mention the disruption of NCIs through cyber means as actions that would give rise to an armed conflict, for instance, but does affirm that "the notion [of armed conflict] clearly requires the existence of hostilities."[216] This means that "state-sponsored cyber operations would give rise to an international armed conflict if they are designed to harm another state [...] also by adversely affecting its military operations or military capacity,"[217] absent of physical damage. The concept of hostilities as criterion for the existence of an armed conflict may enable disruptive cyber operations *severely* affecting the functionality of NCIs to initiate an armed conflict and thus trigger the application of IHL, in that they are able to affect the adversaries military operations without causing physical harm.

While for NIACs the 'armed confrontation' has to reach a minimum level of intensity to qualify as non-international armed conflict itself - it has to be protracted, sustained and large-scale-, in the case of international armed conflict whether or not a certain level of intensity has to be met for the 'resort to armed force' to initiate an armed conflict raises much controversy amongst the international community. In its 2016 Commentary, on Common Article 2 to the four Geneva Conventions, the ICRC affirms that there is no minimum level of intensity for armed force to give rise to an armed conflict, in that:

> "[a]rmed conflicts in the sense of Article 2(1) are those which oppose High Contracting Parties (i.e. States) and occur when one or more States have recourse to armed force against another State, regardless of the reasons for or the intensity of the confrontation."[218]

According to the position of the ICRC, commented by the NATO CCD COE Group of Experts, a cyber operation that targets a small military installation and causes a fire to break out would suffice to give rise to an armed conflict.[219] However, in the cyber context, state practice demonstrates that a certain requirement of intensity is needed for a cyber operation to qualify as 'resort to armed force' under the *jus in bello* and give rise to an international armed conflict, in that "[n]o State is known to have publicly qualified a hostile cyber operation outside an ongoing armed conflict as triggering the applicability of IHL,"[220] despite

---

[215] Nils Melzer, *Cyberwarfare and International Law*, p. 27.

[216] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 383.

[217] Nils Melzer, *Cyberwarfare and International Law*, p. 24.

[218] ICRC, *Commentary of 2016. Article 2: Application of the Convention*. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. para 2 (a) (218).

[219] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 383.

[220] Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations*, p. 71.

the fact that hostile cyber operations in times of peace have occurred. Stuxnet is an example. In case the ICRC's view was to be universally adopted, that is, if there were no minimum requirement of intensity for a cyber operation to amount to 'resort to armed force' and thus give rise to an international armed conflict, and if Stuxnet was attributable to a State, the physical damage caused to the centrifuges at the nuclear fuel processing plant would have triggered the application of LOAC between the responsible State and Iran, as would have happened if the damage to the centrifuges was caused by a kinetic operation. Certainly, this reasoning does not have to be misunderstood, in that a cyber operation causing the destruction of one computer unit would not be considered as 'resort to armed force' and would not trigger the provision of LOAC, as "soldiers throwing a stone at each other [...] would not initiate an international armed conflict."[221] More simply, "the greater the damage, the more likely the situation will be treated as an armed conflict, whatever means are employed to cause the damage."[222]

Going back to disruptive cyber operations that do not cause physical damage or destruction, or injury or death, but that result in loss of functionality of the system targeted, in Roscini's opinion, only those cyber operations that *severely* disrupt the functioning of military or civilian cyber infrastructures could reach the threshold of 'resort to armed force' and be considered as 'belligerent hostilities' triggering the application of LOAC. The cyber operations conducted against Estonia in 2007, for instance, if attributable to Russia, would not have met the threshold of 'resort to armed force' since they did not result in violent effects, and although they targeted NCIs such as the banking and communications infrastructures, they did not result in significant disruption of such NCIs.

To conclude, if cyber operations conducted between two States amount in themselves to 'resort to armed conflict', that is, they are conducted through means and methods of warfare that are able to cause injury or death to people, damage or destruction of objects, or if such cyber operations are able to cause *significant* disruption of NCIs, they can give rise to an international armed conflict.

At the end of the day, the determination of the existence of an armed conflict triggered by cyber operations will be a factual and objective one based on a case-by-case analysis of the

---

[221] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 135.

[222] ibid.

prevailing circumstances that has to be conducted in good faith, often in the hands of international jurisprudence. As a matter of fact, "'[i]f the application of international humanitarian law depended solely on the discretionary judgment of the parties to the conflict, in most cases there would be a tendency for the conflict to be minimized by the parties thereto."[223] It is evident that if a certain situation entails hostile armed actions between States, thanks to Common Article 2(1) to the Geneva Conventions, such Conventions will apply regardless of how States characterize the resort to armed force or an armed confrontation. However, it is necessary to point out that, in lack of an central authority in charge of establishing when an hostile operation - be it kinetic or cyber- amount to armed conflict, the determination of the applicable legal regime to military operations will be conducted by States or parties to the conflict themselves. Evaluations will also be made by the ICRC for the purpose of its work, as established by its Statute and by the Geneva Conventions themselves.

1.2 Cyber Operations and the notion of 'attack' under IHL

After having established when IHL is applicable to cyber operations and before moving the discussion to how the laws of targeting apply to cyber operations, we must understand what the notion of 'attack' entails under IHL in the cyber context.

The notion of 'attack' is fundamental for IHL in that its core principles, namely distinction, proportionality and precaution are expressed in terms of 'attack', that should not be confused or homologated with 'military operations' in that military operations are not subject to the same prohibition and restrictions than attacks. As concluded in Chapter 1, attack is defined by Article 49(1) of AP I, that provides that "attack means acts of violence against the adversary, whether in offence or defence." In the cyber context, the discussion focuses on the classification of cyber operations as 'acts of violence', since it is the 'act of violence' itself that distinguishes an attack from a military operation. Therefore, for a cyber operation to be considered as 'cyber attack' in the sense of LOAC, it has to entail violence. Cyber espionage *per se* or psychological cyber operations, for instance, can be detrimental to the enemy but

[223] ICTR, Akayesu Trial Judgment, 1998, para. 603 in ICRC, *Commentary of 2016. Article 2: Application of the Convention*. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. para 2 (212).

they are not regarded as cyber attacks since they are devoid of violence. It is important to point out that 'acts of violence' should not be intended as activities carried out exclusively through kinetic means. As explained in Chapter 2, it is not the nature of the action, but rather its effects that determine its classification both under the *jus ad bellum* and under the *jus in bello*. Violence, indeed, has to be understood as violent consequences caused by an action. Thus, 'acts of violence', to be considered as such, have to manifest direct consequences as injury of persons, loss of life or tangible damage or destruction of objects.[224] Accordingly, the NATO CCD COE Group of Experts defined 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 of objects."[225]

The definition applies to international and non-international armed conflicts.

There is broad agreement over the characterization of a cyber operation as 'attack' also when injury of persons, loss of life or tangible damage or destruction of objects or a combination thereof are caused *indirectly*. In their commentary to Rule 92 on the definition of cyber attack, the NATO CCD COE Group of Experts stated that the effects that have to be considered should not be limited to those caused directly on the targeted system. They make the example of a cyber operation that infiltrates a SCADA system controlling a dam and manipulates it, leading to the release of waters causing downstream destruction, but that does not damage the targeted system itself.[226] Recalling the taxonomy of effects that result from cyber operations explained in Chapter 1, the manipulation of the SCADA system would be a first-order direct effect, while the downstream destruction would be a second-order effect of the initial cyber operation, and would thus be an *indirect* consequence of the initial act. In the Group of Experts' opinion, that receives broad support from the international community, also second-order (indirect) effects have to be taken into account when classifying a cyber operation as cyber attack. Furthermore, in case the attack is intercepted and the 'reasonably expected violent effects' explained above do not manifest at all or manifest only partially or at a lesser degree, the operation would still be considered an 'attack' in the sense of Article 49(1) of AP I. In its 2019 Position Paper for the UN GGE, the International Committee of the

---

[224] In Chapter 2, I referred to this approach as 'effect-based approach'. The reasoning surrounding this approach can be applied in the classification of cyber operations under International Humanitarian Law as well.

[225] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Rule 92, p. 415.

[226] ibid., p. 416.

Red Cross stated that in its view, the notion of 'attack' "includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack[...]."[227]

Agreement lacks, instead, on the classification as 'attacks' of those cyber operations that capture or neutralize the targeted system, that is to say, that "inhibit, hinder or hamper the proper exercise of its functions rather than kill, injure or destroy the target."[228] The debate focuses on the loss of functionality of an object and argues whether its disruption, rather than its destruction or damage, is sufficient to consider a cyber operation as 'attack'. In its 2019 Report, the ICRC highlighted different approaches to the matter.

A first approach, based on a strict interpretation of the notion of 'attack' as 'act of violence', classifies cyber operations as cyber attacks *only* if they cause injury or death to people and/or damage or destruction of objects. Consequently, it rejects the possibility for a cyber operation to reach the threshold of 'attack' under IHL if its aim is the loss of functionality of an IT system, computer system or computer network. The arguments brought forward to support this point of view are based mostly on Articles 51.5(b),[229] 57.2(a)(iii),[230] and 57.2(b)[231] of AP I, in that, when referring to the proportionality and precaution in *attacks*, prohibit attacks causing injury or loss of lives of civilians and damage or destruction of objects, but they do not prohibit the neutralization of objects. For this reason, under this approach, cyber operations causing the loss of functionality of cyber infrastructure do not amount to attacks.

A second approach evaluates the nature of a given cyber operation based on the actions necessary to restore the functionality of the computer, IT system or object after it has been disrupted. According to this approach, if the restoration of the functions of the object

---

[227] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, ICRC Position Paper submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', November 2019, p. 7.

[228] Nils Melzer, Cyberwarfare and International Law, p. 25.

[229] Article 51.5(b) of AP I defines what attacks are to be considered indiscriminate and that would lack of proportionality. It prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

[230] Article 57 of AP I states the precautions to be taken when launching an attack. In its paragraph 2(a)(iii), it sets forth that States shall "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

[231] Article 57.2(b) "an attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

disrupted by a given cyber operation necessitates the replacement of physical components, the cyber operation in question would be regarded as cyber attack. Since a physical component needs to be replaced, the disruption of the object would amount to damage and would thus rise the cyber operation to the level of cyber attack as intended by IHL. In this regard, it is important to recall that for IHL *de minimis* damage or destruction usually does not meet the required threshold of harm for an operation to be regarded as 'attack'. However, the majority of the NATO CCD COE Group of Experts supported this approach. A minority of them even argued for the extension of the meaning of 'cyber attack' to cyber operations causing interference of functionality that requires not the replacement of physical components, but the "reinstallation of the operating system or of particular data necessary for the targeted cyber infrastructure to perform the function for which it was designed."[232] In their opinion, if the deletion or alteration of data as a result of a cyber operation disrupts the targeted cyber infrastructure so to render impossible the performance of its functions, the cyber operation in question would amount to attack. However, the extension of the notion of cyber attack under IHL to cyber operations causing the disruption of the operating system of the targeted computer or of the data contained therein did not receive support.

The two approaches analyzed so far, and mostly the second one, highlight the limitations imposed by the so-called 'doctrine of kinetic equivalence': a cyber operation that "shuts down the national grid or erases data of the entire banking system of a State would not be an 'attack', while the physical destruction of a server would."[233]

A third approach tries to include disruptive cyber operations into the notion of 'attack' by focusing on the effects that the cyber operation in question has on the functionality of the targeted object. An argument in support of the inclusion of disruptive cyber operations into the notion of 'attack' is given by Dörmann, who argues that in the definition of military objective, Article 52(2) of AP I[234] includes also objects the "capture or neutralization" of

---

[232] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 417.

[233] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 180.

[234] Article 52(2) of AP I states: "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 or *neutralization*, in the circumstances ruling at the time, offers a definite military advantage." In this way, it seems to include also the mere capture or neutralization of objects as forms of attack.

which offers a "definite military advantage."[235] According to Article 52(2) of AP I, also the "capture and neutralization" of military objectives is an action that classifies a military operation as an 'attack'. For this reason, if a cyber operation neutralizes an object by disrupting its functionality, instead of destructing the object itself, the cyber operation in question would amount to a cyber attack even in absence of physical damage or destruction and/or injury or loss of life.

Other approaches could be described but as of today, none of them reaches a solid conclusion or finds consensus among scholars or the international community.

Nowadays, the official position of the ICRC with regard to the matter is that all those cyber operations that are expected to cause death, injury or physical damage are considered 'attacks', be the harm caused directly or indirectly. Furthermore, the ICRC "also considers that an operation designed to disable an object – for example a computer or a computer network – constitutes an attack under the rules governing the conduct of hostilities, whether or not the object is disabled through kinetic or cyber means."[236]

With regard to the opinion of States, not many of them have taken a position on how the notion of 'attack' should apply to cyber operations under the *jus in bello*. The US DoD Law of War Manual intends for cyber attack an operation that "would destroy enemy computer systems,"[237] but not an operation that defaced the website of the government, or that disrupted the internet service for a short amount of time, for instance. Other States, such as Australia, support the application of IHL rules concerning the conduct of attacks to cyber operations that reach the threshold of kinetic attacks under LOAC,[238] recalling the doctrine of kinetic-equivalence mentioned above. Panama, instead, argues that a better way to deal with the issue is that of expanding the notion of 'violence' so to include not only physical damage of objects but also the incapacitation of infrastructure absent of physical destruction.[239] The idea comes from the fact that cyber operations are brought about by the advent of new technologies and, as commented in Chapter 2, such technologies have enabled States to

---

[235] Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, ICRC website, published on November 29th 2004, accessed on June 29th, p. 6.

[236] Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations*, p. 73.

[237] U.S. Department of Defense, *Law of War Manual*, June 2015 (updated December 2016), para 16.5.2, p. 1022.

[238] Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy, October 2017, Annex A, p. 91.

[239] UN General Assembly, Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General, Addendum, A/57/166/ADD.1, 29 August 2002, p. 5.

damage their adversaries without the need to inflict physical harm to objects or people. Furthermore, the more our societies become reliant on computers, computer systems and networks, the more possibilities States will enjoy to damage each other without causing physical harm, and therefore, to circumvent the law on the conduct of hostilities. If the approach advanced by Panama were to be applied, those cyber operations amounting to more than mere inconvenience would reach the level of 'attack' under LOAC. On the contrary, if such position were not to be adopted internationally, the notion of 'attack' would include only those cyber operations that cause injury, death or physical damage, while a cyber operation that aims at disrupting civilian networks - such as electricity- might not be covered by the fundamental provisions of IHL that protect civilian objects and civilians themselves. This last outcome does not seem to be in line with the purpose of LOAC rules on the conduct of hostilities, since it leaves open a wide range of possibilities for States to disrupt, even severely, services essential to civilian life without being subject to the restrictions imposed by IHL, due to the fact that such operations would not qualify as 'acts of violence', and consequently would be left out from many of the restrictions imposed on the conduct of 'attacks'. As of today, it is likely that only multiple and coordinated cyber operations that do not result in physical damage, but that severely disrupt many or all of the national critical infrastructures of a highly digital-dependent State for a long amount of time may be considered to reach the threshold of 'attack'.

For the safeguard of civilians and of civilian objects during armed conflicts, it is fundamental for States to reach a common understanding on what types of cyber operations, apart from the ones causing physical damage or death, classify as 'attack' under IHL, so to serve the purpose of the *jus in bello* and protect civilians from the dangers arising from cyber operations.

2. The Laws of Targeting

Although a cyber operation alone has never initiated an armed conflict, cyber operations have been used during armed conflicts in response to traditional attacks or as preparatory operations to enable kinetic attacks. Like any other military operation, cyber operations and cyber attacks must conform with the laws of targeting and with its main

principles, that are, distinction, proportionality and precaution. Contrary to other military operations, however, cyber operations allow the targeting of specific systems vital to the enemy's war effort and are able to cause severe disruption of everyday life, absent of physical damage. Depending on the interpretation of the notion of 'attack' in relation to cyber operations, certain cyber operations - such as disruptive ones - could fall outside some of the main prohibitions and restrictions of IHL. For this reason, the application of the laws of targeting to the cyber context can prove challenging. On the one hand, recent cyber operations have demonstrated that, thanks to their nature, they are able to disrupt the capacity of a State to provide essential services to its population without causing physical destruction and thus offer new possibilities for States to injure the enemy. The fact that cyber operations often do not result in injury or death or physical damage opens up a new array of possible targets liable of attack which could not be targeted through kinetic means due to excessive collateral damage with respect to the military advantage gained from the operation. On the other hand, given the interconnected nature of military and civilian networks, concerns arise from the fact that cyber weapons could spread uncontrollably to civilian networks. This section will explore how the laws of targeting apply to cyber operations and what are the challenges that arise from the regulation of military operations conducted through the cyber domain.

2.1 Distinction

The principle of distinction is at the heart of the laws of targeting. It is contained in Article 48 of AP I and obliges the parties to an armed conflict to at all times distinguish between combatants and military objectives and civilians and civilian objects and direct their military operations only against the former category. Civilians and civilian objects are protected from attacks by other Articles of AP I, such as Articles 51,[240] 52,[241] and 54.[242] The

[240] Art. 51 of AP I concerns the protection of the civilian population, protects civilians from the dangers arising from military operations and prohibits attacks against civilians.

[241] Art. 52 of AP I prohibits attacks against civilian objects.

[242] Art. 54 of AP I protects those objects considered to be essential for the survival of the civilian population, such as foodstuffs and drinking water installations. It is not only prohibited to attack such objects, but also to destroy, remove or render them useless.

principle of distinction applies to cyber attacks both in international and non-international armed conflicts.[243] For what concerns the protection of persons, legitimate military targets are combatants, members of organized armed groups and civilians directly participating in hostilities, while the civilian population, medical and religious personnel as well as *hors de combat* must be protected and do not constitute legitimate targets of cyber attacks. The cyber realm can pose significant problems in the identification of civilians directly participating in hostilities, or in the identification of the members of irregular armed forces. However, the cyber domain poses even more significant challenges in the targeting of objects. Lawful targets of a cyber attack would be military objectives that, has explained in Chapter 1, are "those objects that for their nature, location, purpose or use make an effective contribution to military action,"[244] or those objects that, if captured or neutralized, offer a definite military advantage. For what concerns their nature, legitimate targets in the cyber realm are those computers designed as components of weapons or weapons systems, for instance.[245] This category of lawful targets can include military networks and databases, weapon systems, battlefield devices, GPS systems, digital communication systems and other military digital systems or devices.[246]

For what concerns their location, legitimate military targets are difficult to identify given the intangible nature of the cyber domain itself. However, depending on the degree of connectivity of a State, a legitimate target could be identified in the "primary connection nodes of a State's internal telecommunications network to the Internet backbone."[247] For what concerns the purpose or use of an object in the cyber context, what marks a computer as military objective is the software installed in it, in that it allows actions that go from the storage of military data, to the encryption or deciphering of codes, to the execution of administrative military tasks.[248] Although for what explained above the identification of a military objective may seem not so difficult, it is important to recall that civilian and military

---

[243] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Rule 93, p. 420-421.

[244] Art. 52 (2) of AP I.

[245] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," *Journal of Conflict and Security Law* vol. 17, no. 2 (2012), p. 263.

[246] Heather Harrison Dinniss, "*The Status and Use of Computer Network Attacks in International Humanitarian Law"*, p. 161.

[247] ibid.

[248] Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," p. 263.

cyber infrastructures are highly interconnected, and that cyberspace itself relies densely on civilian cyber infrastructures. Many military networks, in fact, rely on civilian cyber infrastructures, such as satellites, routers or nodes. Furthermore, civilian logistic supply chains, such as the ones providing food and medical supplies, make use of the same ICT networks used by the military to pass their communications.[249] More frequently than in traditional domains, in fact, military objectives in the cyber realm are likely to be dual-use objects, that is to say, objects that are used both for civilian and military purposes. An example of a cyber dual-use object is a Global Positioning System (GPS), designed initially for military purposes and now integrated in most civilian objects, such as cellphones, laptops, and GPS navigator devices for vehicles. A cyber operation disrupting the service of GPS by blocking its signal may potentially put civilian lives in danger. In this regard, it is important to point out that when an object is dual-use, it becomes a military objective if its use makes an effective contribution to military action, and if the attack would offer a definite military advantage.[250] When such conditions are met, a civilian object losses the protections afforded by many of the rules of LOAC and it is liable of attack. If this understanding was to be applied strictly, "many objects forming part of the cyber infrastructure would constitute military objectives and would not be protected against attack, whether kinetic or cyber."[251] However, in case of doubt as to the nature or use - civilian or military - of the cyber infrastructure targeted, the attacker must refrain from attacking it.[252] Even in the case in which certain civilian cyber infrastructures become military objectives and can be lawfully attacked, any attack against them would have to comply with the prohibition of indiscriminate attacks, as well as with the principles of proportionality and precaution. The assessment of the expected incidental harm that may be caused by the conduct of a certain cyber operation is fundamental for both principles, that will be further discussed in the next sections.

Targets of cyber attacks can be found also outside the cyber domain, in that cyber attacks could be targeting not only softwares or networks, but also physical infrastructures or persons. In this case, in order to establish the lawfulness of a cyber attack, it is fundamental

---

[249] ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts* (2015), p. 42.
[250] Art. 52 (2) of AP I.
[251] ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts* (2015), p. 42.
[252] Art. 52 (3) of AP I.

to determine *which* is the actual object targeted by the cyber attack. Recalling the taxonomy of effects explained in Chapter 1, the aim of a cyber operation could be that of targeting a physical infrastructure outside the IT system, such as an electric power grid. Of course, the expected results on a physical infrastructure could be achieved only as second-order effects. This means that a cyber operation targeting an electric power grid would have to hit first its industrial control system and, only through the infiltration and manipulation of such control system, achieve the expected results on the electric power grid targeted. Therefore, the lawfulness of an attack will also depend on the determination of the relevant object targeted. In the words of Roscini,

> "[w]hen the cyber operation aims to cause material damage to physical property or persons or incapacitation of infrastructures, or such effects are foreseeable, the attacked 'object' is not only, and not mainly, the information itself, but rather the persons, property or infrastructure attacked *through* cyberspace."[253]

Another key issue in the application of the principle of distinction to the cyber domain is whether data can be considered as (civilian or military) 'object' under IHL, and if so, what level of interference, modification, manipulation or damage of civilian data would suffice to qualify an attack as unlawful. The majority of the NATO CCD COE International Group of Experts regarded data as outside the definition of objects, due to their intangibility. Therefore, a cyber operation targeting data would not qualify as attack, unless it affected the functionality of the cyber infrastructure in which the data is stored, or in case it resulted in other consequences that would rise the operation to the threshold of attack.[254] A minority of the Experts, however, argued that data should be regarded as objects subject to the rules of IHL. In their opinion, the deletion of essential civilian assets - as bank accounts, social security data or tax records - would circumvent the restrictions and prohibitions imposed to attacks against civilian objects. Furthermore, they argue that this would be against the general protection to civilians under Article 48 of AP I.[255] Certainly, in case data were to be included in the notion of object, the severity of the consequences manifested by the cyber operation or attack in question would have to be evaluated so to understand to what extent they have breached the proscriptions of IHL. The modification or deletion of civilian data during an attack against military cyber infrastructure, for instance, could amount to 'collateral damage'

---

[253] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 183.

[254] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 437.

[255] ibid.

and consequently the attack would not be unlawful. The same can be said for a cyber espionage operation that manipulates or modifies access data to civilian computers. In this case, the cyber espionage operation would lack of destructive nature and would not constitute an attack under IHL. In this regard, it is important to bear in mind that no cyber operation can be conducted without the deletion or the change of data resident in the system that has been intruded, at least temporarily. For this reason, the classification of data as civilian or as military assets is highly relevant in order to determine the lawfulness of a cyber operation or attack, as well as the severity of the consequences manifested from the deletion or manipulation such data. If data were to be regarded as objects, civilian intangible assets could not be targeted in the first place, granting civilians a fair level of protection also in the cyber domain. The ICRC seems to be in line with the minority of the NATO CCD COE International Group of Experts that are prone to qualify data as objects under IHL. In its 2015 Report, the ICRC observed that "deleting or tampering with data could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects."[256] For such reason, the organization stated that excluding cyber operations against data from the prohibitions and restrictions of IHL does not seem to reconcile with the purpose and object of IHL norms.[257]

Lastly, from the principle of distinction derives the prohibition of indiscriminate attacks, codified in Article 51(4) of AP I. Indiscriminate attacks are those that are not directed at a specific military target or that employ means or methods of combat which cannot be directed at a specific military objective, and those whose effects are not limited and that consequently hit both military objectives and civilian objects without distinction.[258] Cyber operations raise many questions with regard to their capability to targeted specific military objectives, in that some malicious codes, such as viruses and worms, are designed to spread from a computer to another without discrimination. Both viruses and worms can carry payloads able to manifest a set of effects that range from annoyance to the creation of a backdoor for the attacker so to enable him to gain access or control of the computer

[256] ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts* (2015), p. 43.
[257] ibid.
[258] Art. 51(4) of AP I.

compromised by the malicious code.[259] The malicious code could also be designed to cause effects that would rise the cyber operation to the threshold of attack, and would thus be unlawful also in this regard. However, further examination of a variety of cyber tools has demonstrated that they are not necessarily indiscriminate. As explained in the ICRC Position Paper for the UN GGE, "[m]any of the recent cyber attacks that have been reported in public sources appear to have been rather 'discriminate' from a technical point of view: they have been designed and actually used to target and harm only specific objects and have not spread or caused harm indiscriminately."[260] However, making sure that cyber tools do not spread uncontrollably can prove challenging and their design and use requires a great amount of preparation and planning.

2.2 Proportionality

Although attacks against civilians and civilian objects are prohibited, civilians may be hit incidentally as 'collateral damage' of an attack - cyber or kinetic - that had targeted a military objective. For this reason, the principle of distinction is moderated by the principle of proportionality, that attempts to balance the incidental injury of civilians or damage of civilian objects with the military advantage gained as a result of the attack. The principle is applicable to cyber attacks, and it was transposed to the cyber domain in the *Tallinn Manual 2.0* as follows:

> "[a] cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited."[261]

Rule 113 of the *Tallinn Manual 2.0* is based on Articles 51(5)(b) and 57(2)(iii) of AP I, that codify the rule of proportionality. Due to the interconnected nature of military and civilian cyber infrastructures, the principle of proportionality plays a crucial role in the cyber context, since many civilian cyber infrastructures may become military objectives and be liable of

---

[259] Heather Harrison Dinniss, "*The Status and Use of Computer Network Attacks in International Humanitarian Law"*, p. 176.

[260] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (2019), p. 5.

[261] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Rule 113, p. 470.

attack. Reduced to basics, the principle attempts to balance two elements: 1) incidental damage to civilians or civilian objects; 2) the concrete and direct military advantage anticipated from the attack. In the cyber context, a commander, before launching a cyber attack will have to consider not only the first-order effects, but also the second-order effects expected to result from the initial cyber attack. An example of cyber attack which is likely to cause collateral damage is that against a Global Positioning System. As explained above, the object is dual-use and thus a lawful target of attack. However, the disruption of the service would not be the only effect of the cyber attack, in that the attack is likely to cause also injury or death of civilians and damage or destruction of objects, due to the fact that civilian aircrafts rely on the system, for instance. If the expected harm to civilians or civilian objects exceeds the anticipated direct and concrete military advantage of the cyber attack, such attack would be prohibited. On the contrary, if cyber operations cause "inconvenience, irritation, stress, or fear,"[262] such effects on the civilian population would not be considered as 'collateral damage' since they do not amount to incidental loss of civilian life, injury to civilians or damage to civilian objects.

Lastly, it is important to recall that 'damage to civilian objects' includes also the loss of functionality of such objects, if the disruption of cyber infrastructures is included in the definition of attack. Consequently, also the loss of functionality of a civilian cyber infrastructure has to be considered in the proportionality test for the determination of the lawfulness of a cyber attack.

2.3 Precaution

Article 57 of AP I sets out the obligation for an attacker to take all feasible precautions in order to verify that the targeted object is a military objective and to avoid or at least minimize the collateral damage expected to civilians and civilian objects. Article 58 of the same Protocol, instead, obliges the belligerents to protect their civilians from the effects of an attack. The principle of precaution is recognized as customary international law and as

[262] ibid., p. 472.

such, it applies to the cyber domain. This principle is very relevant in the cyber context due to the interconnected nature of networks.

The obligation to take precautions when launching an attack can be summarized in three elements: 1) the attacker has to verify the nature of the targeted object with some degree of certainty; 2) the attack has to be directed against that specific target; 3) the choice of means and methods to conduct the operation has to be in accordance with the principle of proportionality, so to avoid or at least minimize the incidental damage inflicted to civilians and civilian objects.[263] The application of the first element to the cyber domain entails that the attacker, when planning the attack, will have to map the network targeted with a high level of accuracy through cyber exploitation operations, so to make sure that the targeted network is a military objective. Due to the nature itself of the planning of a cyber attack, that requires extensive system scanning and surveillance in order to determine how to infiltrate into the targeted system, this element is thought to be quite easy to comply with. The second element concerns the execution of the cyber attacks, and implies that specialized personnel should be in charge of the conduct of the cyber attack so to make sure that it hits the targeted military objective only. If no specialized personnel is available at the time in which the attack should be launched, the attacker should refrain from launching the attack. This element, instead, proves to be more problematic in the conduct of cyber attacks, in that military commanders are not expected to have a solid knowledge of all the targets they attack, and for this reason, they often rely on reports made by their military intelligence. However, it is well established that military commanders should take their decisions on the basis of the information that is available at the time of the attack, be it kinetic or cyber.[264] The third element requires the attacker to choose means and methods for the conduct of the attack that will minimize incidental damage to civilians. In this regard, cyber attacks are often preferred with respect to kinetic attacks, in that entail lower risks of causing collateral damage and consequently they are thought to have a lower impact on the civilian population.

In the cyber context, the obligation for belligerents to protect their civilians from the effects of an attack, also referred to as passive precautions, would require belligerents to distinguish and separate civilian computer data, civilian networks and systems, and civilian cyber

---

[263] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 234.

[264] Heather Harrison Dinniss, "*The Status and Use of Computer Network Attacks in International Humanitarian Law"*, p. 181.

infrastructure from the military one, for instance. The obligation could also entail the physical separation of the hardwares on which civilian systems and networks rely. However, due to the interconnected nature of cyberspace, this could prove difficult to implement, in that military communications and information often pass through civilian networks and also through civilian information infrastructures, such as fibre-optic cables or servers. Nowadays, for the sustained financial costs and for technical difficulties, the separation of military and civilian networks and information infrastructure is not believed to be possible. However, what can surely be done at present to comply with the obligation of passive precautions is the massive use of cyber defence, for instance, and other standard measures of the so-called 'cyber-hygiene', such as the installation of anti-viruses capable of intercepting malicious codes and frequent back-ups to allow data recovery.

Conclusions

Given the lack of a legal binding document at international level that regulates the conduct of cyber operations both in times of peace and in times of war, the aim of this dissertation was that of wondering whether existing international law on the use of force, on self-defence and on the conduct of hostilities is applicable to cyber operations, and if so, how. In order to determine what stated above, firstly it was fundamental to analyze the interpretative quandaries that still surround the traditional notions of 'use of force' and of 'armed attack' under the *jus ad bellum*, and the notion of 'attack' under the *jus in bello.* Furthermore, it was necessary to identify what is meant for cyber operation, for cyber attack and for cyber warfare. A study on cyber weapons, what they entail, how they work and their effects was the key for approaching critically the dilemma of the application of *de lege lata* to the cyber context.

Secondly, it was necessary to determine whether cyber operations, given their non-kinetic nature, can be classified as 'use of force' under Article 2(4) of the UN Charter, as 'armed attack' triggering the right of self-defence under Article 51 of the same Charter, and whether cyber operations amount to 'attack' or to 'resort to armed force' so to trigger the application of the laws on the conduct of hostilities.

For what concerns the *jus ad bellum*, it was found that both Article 2(4) and Article 51 of the UN Charter are applicable to cyber operations, in that they are recognized as customary international law and their application is not limited to the use of 'armed force' only. In the *Nicaragua* judgement, in fact, the ICJ suggested that other forms of 'force' distinct from 'armed force' can be identified. The fact that cyber operations are not carried out through traditional means does not represent an obstacle when it comes to their regulation under the prohibition on the use of force and their classification as 'armed attack'. Both Article 2(4) and Article 51 of the UN Charter apply to any use of force, regardless of the weapon employed. In order to determine when an action can be considered use of force, the ICJ distinguished between the 'most grave forms' of the use of force - that is to say, those uses of force that amount to armed attack - and the 'less grave forms'. Instead of focusing on the nature of the action, the Court focused on its scale and effects, suggesting that the

traditional instrument-based approach for the identification of an action as 'use of force' could be substituted by, or at least complemented with, the effect-based approach. The effect-based approach classifies an action according to the effects it manifests, instead of focusing on the instrument used for its execution. Such approach is thought to be the most suitable when it comes to the classification of cyber operations as 'use of force' or as 'armed attack'. Following this approach, all those cyber operations that result in injury or death of persons, damage or destruction of objects can be considered use of force in breach of Article 2(4) of the UN Charter and reach the threshold of armed attack - 'most grave forms of use of force'. Consequently, they can trigger the right of-self defence under Article 51 of the UN Charter. Cyber operations, indeed, have already demonstrated to have the potential to cause at least destruction of objects and it is known that they have also the potential of causing injury and loss of human lives. Certainly, the cyber operations in question would have to be conducted by or be otherwise attributable to a State and conducted against another State.

What is still unclear is whether those cyber operations that do not result in injury or death and/or damage or destruction, but that cause severe disruption, can qualify as use of force. If one recurs to traditional uses of force - non-cyber -, it has been shown that even the training and the arming of the *contras* in the *Nicaragua* case amounted to use of force. In the same way, cyber operations causing disruption instead of destruction could amount to use of force. In this regard, the challenge lies in the fact that the effects of cyber operations range from mere inconvenience to death or injury of persons; moreover, they can affect social, economic, physical or physiological security by disrupting NCIs. Hence, the use of force demarcation line must be placed somewhere in between economic or diplomatic coercion and the use of force reaching the threshold of armed attack. A suitable way to determine whether a non-destructive cyber operation can amount to use of force is thought to be that of classifying the nature of their consequences according to the criteria advanced by Michael N. Schmitt in 1999 and revised by the NATO CCD COE International Group of Experts in 2017. If the consequences of a cyber operation approximate the consequences that characterize armed force - measured in terms of severity, immediacy, directness, invasiveness, measurability (of effects), presumptive legitimacy, military character and state involvement - the cyber operation in question would amount to use of force.[265] Cyber operations that do not manifest

[265] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,"p. 915.

effects that approximate those caused by conventional uses of force - death or injury of persons, damage or destruction of objects, or *severe* disruption of NCIs following Schmitt's criteria - would not be considered uses of force. They may amount, instead, to unlawful intervention in another State's internal affairs, for instance. Due to the fact that there is no univocal answer to whether cyber operations amount to use of force, and in lack of a precise line of demarcation in the 'spectrum of consequentiality' that indicates where to locate the use of force carried out within the cyber domain, the most suitable option is that of a case by case assessment. While cyber operations continue to be used by States in their international relations, State practice and international jurisprudence will surely clarify some of the dilemmas that still remain open.

Having established that a cyber operation amounts to armed attack when it causes injury or death to persons, damage or destruction of objects, the analysis of this dissertation moved to exploring *how* the right of self-defence could be applied to the cyber context. The findings of Chapter 2 lead to the conclusion that the right of self-defence can be exercised to repel or stop a cyber attack. Its application, however, proves to be challenging for several reasons. Cyber attacks are often 'multi-layered', that is to say, a single cyber attack may be composed of different cyber actions. In this case, it is important to determine which cyber action constitutes the armed attack triggering the forceful response. Therefore, does the cyber attack begin with the cyber action that infiltrates the targeted system or does it begin when it executes its payload, or even when its effects manifest? On the one side, if a cyber attack is intended as the sum of the cyber actions needed to execute it and manifest its intended effects, the cyber attack would begin from the moment it infiltrates the targeted system, and therefore it would trigger the right of self-defence from that moment. However, in this case, the principles of necessity and proportionality would be difficult to apply given that the 'scale and effects' of the cyber attack are unknown. On the other side, if a cyber attack is intended as such from the moment in which it manifests its effects, the attack would begin to exist when its destructive effects manifest, regardless of when the targeted system had been infiltrated or of when the payload had been executed. No agreement has been reached yet on the matter.

When talking about self-defence against a cyber attack, it is important to take into account that they often do not come alone: a cyber operation or a cyber attack may be the prelude of a

conventional armed attack. For the purpose of self-defence, when a cyber operation is used to prepare the road for a conventional attack, the notion of interceptive self-defence may prove useful. The right to use force in self-defence also arises if a cyber armed attack is imminent.[266] Anticipatory self-defence can be used in response to a cyber attack in two scenarios: when a cyber attack is expression of an imminent threat of a traditional armed attack; and when electronic activity shows that a cyber armed attack is imminent. In the first scenario, the assessment of the target of the traditional attack will be of great relevance for the purpose of anticipatory self-defence. If the preparatory cyber attack targets NCIs, such as early warning systems, or military communications, or emergency response systems, it will be more likely that the victim State will consider the upcoming traditional attack as imminent, and therefore that such State will act in anticipatory self-defence. In the second scenario, the lawfulness of a response in anticipatory self-defence is harder to assess since the victim State, after having detected that its computer systems have been infiltrated and compromised with a malware, would not have sufficient evidence as to whether a cyber armed attack will take place, nor of its intensity and magnitude. In absence of evidence, the principles of necessity and proportionality would not be satisfied, and neither would the requirement of imminence. Consequently, acting in anticipatory self-defence would not be in order. Anticipatory self-defence against an imminent cyber armed attack alone is considered to be very difficult to invoke. In fact, in lack of evidence concerning the originator of the attack, the nature of the attack itself and its imminence, the necessity and the proportionality of the response in anticipatory self-defence would be nearly impossible to assess. Consequently, what is evident is that so far cyber defense must rely mostly on automated systems for the detection of and protection from cyber attacks.

After having determined if and how cyber operations could be governed by the *jus ad bellum*, the third Chapter of this dissertation focused on whether cyber operations can be regulated by International Humanitarian Law during international or non-international armed conflicts. As of today, it seems uncontested that IHL applies to cyber operations carried out during armed conflicts. This view is confirmed by the ICJ, that stated that "the employment of cyber capabilities in armed conflicts must comply with all the principles and rules of IHL,

---

[266] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, p. 350.

as is the case with any other weapon, means or method of warfare, new or old."[267] Certainly, for IHL to apply, cyber operations must have a 'belligerent nexus' with the ongoing armed conflict or otherwise be related to it.

Successively, it was also wondered whether cyber operations *alone* can amount to 'resort to armed force' and thus give rise to an armed conflict. The challenge lied in determining whether cyber attacks that cause or are likely to cause injury or death of persons, damage or destruction of objects, and thus amounts to 'armed attack' under the *jus ad bellum*, suffice to be considered 'resort to armed force' under the *jus in bello* and thus give rise to an armed conflict. The position of the ICRC on the matter is affirmative, as it clearly stated that a cyber operation causing the death or injury of combatants or civilians or resulting in the destruction of civilian or military objects, or a combination thereof, should not be treated differently from conventional attacks that result in the same consequences.[268] However, State practice demonstrates that not all uses of armed force necessarily lead to the outbreak of an armed conflict and that a certain degree of intensity is required for a cyber operation to qualify as 'resort to armed force' under the *jus in bello* so to give rise to an armed conflict. In fact, the greater is the damage caused by an operation, the higher are the chances that the situation will be treated as an armed conflict, regardless of the means that were employed to inflict the harm. For what concerns cyber operations that do not result in physical destruction, only those cyber operations that result in the *severe* disruption of the functioning of military or civilian cyber infrastructures could reach the threshold of 'resort to armed force' and could be considered as 'belligerent hostilities' triggering the application of LOAC.

Finally, it was found that cyber operations can amount to 'attack' within the meaning of International Humanitarian Law when they cause - directly or indirectly - injury or death to persons and/or damage or destruction of objects. Cyber attacks would thus be subject to the prohibitions and restrictions applied to the conduct of 'attacks' by the laws of targeting. With regard to cyber operations that do not result in physical damage, it is likely that only multiple and coordinated cyber operations that severely disrupt several NCIs of a highly digitalized State for a long period of time may be considered to reach the threshold of 'attack'.

---

[267] ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts*, (2015), p. 40.

[268] Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations*, p. 71.

The application of the laws of targeting to the cyber context, especially the application of the principles of distinction, proportionality and precaution encounters difficulties coming from the very nature of this man-made domain. In order to assure the protection of civilians and of civilian objects from the dangers arising from cyber operations, it is urgent that such difficulties are overcome.

Despite the growing attention on the topic, the international community has failed to reach agreement on how to define the terms of the cyber realm, and consequently, on how to regulate the conduct of cyber operations both in times of peace and in times of armed conflict. At present, there is still no official or agreed definition of cyber operation, of cyber attack and of cyber warfare, nor there is a proposal for a binding document at international level that regulates the use of force in cyberspace in all its declinations. The lack of agreed definitions comes from different political perspectives and policy concerns on the matter, that States will hopefully overcome thanks to the holding of annual forums of discussion on cyber security-related issues. For the moment, what argued in this final dissertation remains only theoretical. State practice and international jurisprudence will surely advance the adaptation of *de lege lata* to cyber operations or will find alternative ways to regulate the conduct of cyber operations. How? Time will tell.

Reference List

1. Books

Alexandrov, Stanimir A. *Self-Defense Against the Use of Force in International Law*. The Hague: Kluwer Law International, 1996.

Amoroso, Amoroso and Guglielmo Tamburrini. 'Filling the Empty Box: A Principled Approach to Meaningful Human Control over Weapons Systems', *ESIL Reflections* Vol 8, No. 5 (2019): 1-9.

Arend, Anthony Clark and Robert J. Beck. *International Law and the Use of Force: Beyond the U.N. Charter Paradigm*. London and New York: Routledge, 1993.

Arimatsu, Louise. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." in *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, K. Ziolkowski, 91-109. Tallinn: 2012 NATO CCD COE Publications, 2012.

Baradaran, Nazanin and Homayoun Habibi. "Cyber Warfare and Self-Defense from the Perspective of International Law." *Journal of Politics and Law* Vol.10, No. 4 (2017): 40-54. Doi:10.5539/jpl.v10n4p40

Borghard, Erica D. & Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* Vol. 26, No. 3 (2017): 452-481. Doi: 10.1080/09636412.2017.1306396

Caton, Jeffrey L. *Distinguishing acts of war in cyberspace: assessment criteria, policy considerations, and response implications*. Strategic Studies Institute and U.S. Army War College Press. October 2014.

Constantinou, Avra. *The Right of Self-Defence Under Customary International Law and Article 51 of the United Nations Charter.* Athènes: Sakkoulas, 2000.

Crowther, Glenn Alexander. "The Cyber Domain." *The Cyber Defense Review* Vol. 2, No. 3 (2017): 63–78. www.jstor.org/stable/26267386

Dale, Peterson. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* Vol.36, No. 1 (2013): 120-124. Doi: 10.1080/01402390.2012.742014

Devai, Dóra. "Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-proliferation Assumptions." *AARMS* Vol. 15, No. 1 (2016): 61-73.

DeWeese, Geoffrey S. "Anticipatory and Preemptive Self-Defence in Cyberspace: The Challenge of Imminence." in *2015 7th Conference on Cyber Conflict: Architectures in Cyberspace*, edited by. M.Maybaum, A.M.Osula, 81-92. Tallinn: 2015 NATO CCD COE Publications, 2015.

Diamon, Eitan. "Applying International Humanitarian Law to Cyber Warfare." In *Law and National Security: Selected Issues*, edited by Pnina Sharvit Baruch and Anat Kurz, 67-84. Tel Aviv: Institute for National Security Studies, 2014. www.jstor.org/stable/resrep08957.8

Dinniss, Heather Harrison. "The Status and Use of Computer Network Attacks in International Humanitarian Law." PhD diss., London School of Economics and Political Science, 2008.

Dinstein, Yoram. "The Principle of Distinction and Cyber War in International Armed Conflicts." *Journal of Conflict and Security Law* Vol. 17, No. 2 (2012), 261–277. Doi: 10.1093/jcsl/krs015

Dinstein, Yoram. *The Conduct of Hostilities under the Law of Armed Conflict*. Cambridge: Cambridge University Press, 2010.

Farewell, James P. and Rafal Rohozinski. “The New Reality of Cyber War.” *Survival* No. 54, Vol. 4 (2012): 107-120. Doi: 10.1080/00396338.2012.709391

Finlay, Lorraine and Christian Payne. “Symposium on Cyber Attribution: The Attribution Problem and Cyber Armed Attacks.” *AJIL UNBOUND* Vol. 113, (2019): 202-206. Doi: 10.1017/aju.2019.35

Gaggioli, Gloria. "The Use of Force in Armed Conflicts Conduct of Hostilities, Law Enforcement, and Self-Defense." in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare,* edited by Winston S. Williams, and Christopher M. Ford. New York: Oxford University Press, 2019. Oxford Scholarship Online, 2018. Doi: 10.1093/oso/9780190915360.003.0003.

Gray, Christine. *International Law and the Use of Force*. New York: Oxford University Press, 2004.

Gray, Christine. “The use of force and the international legal order”, in *International Law*, edited by Malcolm D. Evans, 601- 631. New York: Oxford University Press, 2018 (Fifth edition).

Greenwood, Christopher. “The Concept of War in Modern International Law.” *International and Comparative Law Quarterly* Vol. 36, No. 2 (1987): 238-306. doi:10.1093/iclqaj/36.2.283.

Hemme, Kris. "Critical Infrastructure Protection: Maintenance is National Security." *Journal of Strategic Security* Vol. 8, No. 3 Suppl. (2015): 25-39.

Henry, W.C., et al. “Pearl Harbor 2.0: When Cyber-Acts Lead to the Battlefield.” *Journal of Information Warfare* Vol. 9, No. 2 (2010): 47–56. www.jstor.org/stable/26486787.

Inkster, Nigel.“Information Warfare and the US Presidential Election.” *Survival* Vol. 58, No. 5 (2016): 23-32. Doi: 10.1080/00396338.2016.1231527

Junio, Timothy J. “How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate.” *Journal of Strategic Studies* Vol. 36, No. 1 (2013): 125-133. Doi: 10.1080/01402390.2012.739561

Kesser, Oliver and Wouter Werner. “Expertise, Uncertainty, and International Law: A Study on the Tallinn Manual on Cyberwarfare.” *Leiden Journal of International Law* Vol. 26, No. 4 (2013): 793-810. Doi: https://doi.org/10.1017/S0922156513000411

Kingsbury, Heather. “International Laws Applicable to Cyber-Warfare.” Master’s diss., Utica College, 2014.

Koh, Harold. “International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012.” *Harvard International Law Journal Online* Vol. 54, (December 2012): 1-12. https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf

Krepinevich, Andrew F. *Cyber Warfare: A “Nuclear Option”?*.Center for Strategic and Budgetary Assessments, 2012.

Libicki, Martin C. *Cyberdefence and Cyberwar*. Rand Corporation. 2009.

Libicki, Martin C. “Why Cyber War Will Not and Should Not Have Its Grand Strategist.” *Strategic Studies Quarterly* Vol. 8, No. 1 (Spring 2014): 23- 39. www.jstor.org/stable/26270603

Liles, Samuel, Marcus Rogers, J. Eric Dietz, Dean Larson. “Applying Traditional Military Principles to Cyber Warfare.” in *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, K. Ziolkowski, 169-180. Tallinn: 2012 NATO CCD COE Publications, 2012.

Martino, Luigi. “La quinta dimensione della conflittualità. L’ascesa del cyberspazio e i suoi effetti sulla politica internazionale.” *Il Mulino - Rivisteweb* Vol.1, (gennaio-aprile 2018): 61-76. doi: 10.4476/89790

Mavropoulou, Elizabeth. “Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks.” *Journal of Law & Cyber Warfare* Vol. 4, No. 2 (2015): 22-93. www.jstor.org/stable/26441253

Mele, Stefano. "Legal Considerations on Cyber-Weapons and Their Definition." *Journal of Law & Cyber Warfare* Vol. 3, No. 1 (2014): 52-69. www.jstor.org/stable/26432559.

Melzer, Nils. *Cyberwarfare and International Law*. UNIDIR Resources, 2011. https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

Melzer, Nils. “The Principle of Distinction under International Humanitarian Law.” in *Targeted Killing in International Law*, 300-366. Oxford: Oxford University Press, 2008.

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel. “The Law of Cyber-attacks.” *California Law Review* Vol. 100, No. 4 (August 2012): 817-885. https://www.jstor.org/stable/23249823

Orye, Erwin and Olaf M. Maennel. “Recommendations for Enhancing the Results of Cyber Effects.” in *2019 11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky, 1-19. Tallinn: 2019 NATO CCD COE Publications, 2019.

Pomès, Eric. “Technological Innovations and International Humanitarian Law: Challenges and Tensions.” *Polish Political Science Yearbook* Vol. 46, No. 2 (2017): 205–223. Doi: 10.15804/ppsy2017213

Pool, Phillip. “War of the Cyber World: The Law of Cyber Warfare.” *The International Lawyer* Vol. 47, No. 2 (2013): 299–323. www.jstor.org/stable/43923953

Porro, Giuseppe and Ornella Porchia. *Studi di Diritto Internazionale Umanitario*. Torino: G. Giappichelli, 2004.

Program on Humanitarian Policy and Conflict Research at Harvard University. *HPCR Manual on International Law Applicable to Air and Missile Warfare*. Cambridge: Cambridge University Press, 2013.

Rid, Thomas and Peter McBurney. “Cyber-Weapons.” *The RUSI Journal* Vol. 157, No. 1 (2012): 6-13. Doi:10.1080/03071847.2012.664354

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* Vol. 38, No. 1 (2015): 4-37. Doi: 10.1080/01402390.2014.977382

Ronzitti, Natalino. *Introduzione al Diritto Internazionale*. Torino: G. Giappichelli Editore, 2013 (Quarta Edizione).

Ronzitti, Natalino. *Diritto Internazionale Dei Conflitti Armati*. Torino: Giappichelli, 2011 (Quarta Edizione).

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014. Oxford Scholarship Online, 2014. Doi: 10.1093/acprof:oso/9780199655014.001.0001

San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994. https://www.legal-tools.org/doc/118957/pdf/

Schmitt, Michael N. "*"Attack" as a Term of Art in International Law: The Cyber Operations Context"*, in *2012 4th International Conference on Cyber Conflict*, edited by. C. Czosseck, R. Ottis, K. Ziolkowski, 283 - 293. Tallinn: NATO CCD COE Publications, 2012.

Schmitt, Michael N. "Classification of Cyber Conflict." *Journal of Conflict & Security Law* Vol. 17, No. 2 (2012): 245-260. Doi:10.1093/jcsl/krsOl8.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* Vol. 37 (1998-99): 885-937. https://ssrn.com/abstract=1603800

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*. New York: Cambridge University Press, 2017.

Schmitt, Michael N. "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations." *International Review of the Red Cross: Memory and War* Vol. 101, No. 1 (2019): 333–355. Doi:10.1017/S1816383119000018

Schulze, Matthias. "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations." in *2020 12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindoström, M. Signoretti, I. Tolga, G. Visky, 183 - 197. Tallinn: NATO CCD COE Publications, 2020.

Tsagourias, Nicholas. "Cyber attacks, self-defence and the problem of attribution." *Journal of Conflict & Security Law* Vol. 17, No. 2 (2012): 229–244. Doi:10.1093/jcsl/krs019

Turns, David. “The Law of Armed Conflict (International Humanitarian Law).” in *International Law*, edited by Malcolm D. Evans, 840- 875. New York: Oxford University Press, 2018 (fifth edition).

United States Department of Defence, “Information Operations: The Fifth Dimension of Warfare. Remarks as delivered by Gen. Ronald R. Fogleman, Air Force chief of staff, to the Armed Forces Communications-Electronics Association, Washington, April 25, 1995.” *Defense Issues* Vol. 10, No. 47 (1995).

United States Department of Defense, *Law of War Manual*. June 2015 (updated December 2016).

Voitasec, Dan-Iulian. “Applying International Humanitarian Law to Cyber-Attacks.” *Lesij* No. XXII, Vol. 1/2015 (2015): 124-131.

Wallace, David and Shane R. Reeves. “The Law of Armed Conflict’s “Wicked” Problem: Levée en Masse in Cyber Warfare.” *International Law Studies* Vol. 89 (2013): 646-668.

Woltag, Johann-Christoph. “Cyber Warfare,” in *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law*, edited by Frauke Lachenmann and Rüdiger Wolfrum, 313 - 321. New York: The Max Planck Foundation for International Peace and the Rule of Law and Oxford University Press 2017, 2017 (First Edition).

Zemanek, Karl. “Armed Attack”, in *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law*, edited by Frauke Lachenmann and Rüdiger Wolfrum, 26 - 31. New York: The Max Planck Foundation for International Peace and the Rule of Law and Oxford University Press 2017, 2017 (First Edition).

2. Online Official Papers and Reports

Cabinet Office. *Public Summary of Sector Security and Resilience Plans 2017.* London: December 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Australia's International Cyber Engagement Strategy.* October 2017. https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf

Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs. Commanders of the Combatant Commands. Directors of the Joint Staff Directories. *Joint Terminology for Cyberspace Operations.* November 2011.

Gisel, Laurent and Lukasz Olejnik. *The Potential Human Cost of Cyber Operations*. ICRC Expert Meeting. ICRC Reports, Geneva, 14-16 November 2018.

High Representative of the European Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 7 February 2013.

ICRC. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. Geneva, 2009 (prepared by Nils Melzer). http://www.icrc.org/eng/resources/documents/publication/p0990.htm

ICRC. *International Humanitarian Law and Cyber Operations during Armed Conflicts*. ICRC Position Paper submitted to the 'Open-Ended Working Group on Developments in the

Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. November 2019. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

ICRC. *International Humanitarian Law and the challenges of contemporary armed conflicts.* ICRC Reports. 32nd International Conference of the Red Cross and the Crescent. Geneva, 2015.

ICRC. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Recommitting to the Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions.* October 2019.

Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12. 8 June 2018.

Ministero delle Comunicazioni, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione. *Network Security in critical infrastructures.* Roma, PrintArt. http://www.isticom.it/documenti/news/pub_003_eng.pdf

Moteff, John, Claudia Copeland and John Fischer. *Critical Infrastructures: What Makes an Infrastructure Critical?* Congressional Research Service Report, 29 January 2003. https://fas.org/irp/crs/RL31556.pdf

National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities*, edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin. 2009. https://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf

North Atlantic Treaty Organization. *NATO Glossary of Terms and Definitions in English and French*. *Glossaire OTAN de termes militaires et definitions en englais et française.* NATO Standardization Office (NSO). AAP-06 Edition 2019. 2019.

Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security. Collated Summaries. 12 March 2019.

Sistema di Informazione per la Sicurezza della Repubblica. *Documento di sicurezza nazionale in Relazione sulla politica dell'informazione per la sicurezza 2018.* Presidenza del Consiglio dei Ministri. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf

The Ministry of Foreign Affairs of the Russian Federation. *Doctrine of Information Security of the Russian Federation*. Approved by Decree of the President of the Russian Federation No. 646 of 5 December 2016. 5 December 2016. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Theohary, Catherine A. and John W. Rollins. *Cyberwarfare and Cyberterrorism: In Brief.* Congressional Research Service. CRS Report. 27 March 2015.

United Nations Office for Coordination of Humanitarian Affairs (OCHA). *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies*. OCHA Policy and Studies Series. October 2014.

United Nations Secretary-General, Australia, Belarus, Brunei Darussalam, Cuba, Oman, Qatar, Russian Federation, Saudi Arabia, United Kingdom, United States. *Developments in the field of information and telecommunications in the context of international security : report of the Secretary-General.* UN Doc A/54/213. 10 August 1999.

United States. *DoD Dictionary of Military and Associated Terms.* January 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

United States Department of Defense. *National Military Strategy for Cyberspace Operations.* December 2006. https://www.hsdl.org/?view&did=35693

United States Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 8 November 2010 (As Amended Through 15 February 2016). https://fas.org/irp/doddir/dod/jp1_02.pdf

3. Conventions, Treaties, Resolutions and Directives

Convention for the Pacific Settlement of International Disputes (Hague, I). The Hague, 29 July 1899, entry into force 4 September 1900.

Convention relative to the Opening of Hostilities (Hague III). The Hague, 18 October 1907, entry into force 26 January 1910.

Convention respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (Hague IV). The Hague, 18 October 1907, entry into force 26 January 1910.

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, entry into force 21 October 1950.

Covenant of the League of Nations, 20 April 1919, entry into force 10 January 1920.

Council of the European Union, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. 8 December 2008.

Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (A/8082). A/RES/2625 (XXV). 24 October 1970.

European Union. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* 6 July 2016.

General Treaty for Renunciation of War as an Instrument of National Policy. Paris, 27 August 1929, entry into force 25 July 1929.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, entry into force 7 December 1978.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, entry into force 7 December 1978.

Shanghai Cooperation Organization. *Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*. 61st Plenary Meeting. 2 December 2008.

Treaty of friendship, co-operation and mutual assistance between the People's Republic of Albania, the People's Republic of Bulgaria, the Hungarian's People's Republic, the German Democratic Republic, the Polish People's Republic, the Romanian People's Republic, the Union of Soviet Socialist Republics and the Czechoslovak Republic. Warsaw, 14 May 1955, entry into force 6 June 1955.

The *Inter-American Treaty of Reciprocal Assistance and Final Act of the Inter-American Conference for the Maintenance of Peace and Security.* Rio de Janeiro, 2 September 1947, entry into force 3 December 1948.

The North Atlantic Treaty Organization. *The North Atlantic Treaty.* Washington D.C., 4 April 1949, entry into force 24 August 1949.

United Nations. *Charter of the United Nations and Statute of the International Court of Justice.* San Francisco, 1945, entry into force 24 October 1945.

United Nations General Assembly. *Definition of Aggression.* A/RES/3314 (XXIX). 14 December 1974.

United Nations General Assembly. *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General*, Addendum. A/57/166/ADD.1. 29 August 2002.

UN General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General.* A/70/174. 22 July 2015.

5. Jurisprudence

International Court of Justice. *Legality of The Threat or Use of Nuclear Weapons*, *Advisory Opinion.* ICJ Reports 1996.

International Court of Justice. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States).* Merits, Judgement of 27 June 1986, ICJ Reports 1986.

International Criminal Tribunal for the former Yugoslavia. *Prosecutor v Duško Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Interlocutory Appeal). Case No IT-94-1-AR72, 2 October 1995.

6. Websites

Bar-On, Anat E. "Cyber-attack and the Prohibition of the Use of Force: The scope of Article 2(4) in Cyberspace." The Hebrew University of Jerusalem. Accessed 20 November 2020. https://csrcl.huji.ac.il/book/cyber-attack-and-prohibition-use-force-scope-article-24-cyberspace

Bertolini, Gianluca. "Il (Dis)ordine Mondiale: Le manovre di Usa, Cina e Russia alla conquista della quinta dimensione." Opinio Juris Law & Politics Review. Published 2 July 2019. Accessed 20 November 2020. https://www.opiniojuris.it/il-disordine-mondiale/

Center for the Protection of National Infrastructure. "Critical National Infrastructure." Accessed 14 May 2020. https://www.cpni.gov.uk/critical-national-infrastructure-0

Cybersecurity and Infrastructure Security Agency. "Critical Infrastructure Sectors." Last modified 24 March 2020. Accessed 14 May 2020. https://www.cisa.gov/critical-infrastructure-sectors

Dörmann, Knut."Applicability of the Additional Protocols to Computer Network Attacks." ICRC Website. Published 29 November 2004. Accessed 29 June 2020. https://www.icrc.org/en/doc/resources/documents/misc/68lg92.htm

Durham, Helen. “Cyber operations during armed conflict: 7 essential law and policy questions.” Humanitarian Law & Policy. Published 26 March 2020. Accessed 18 June 2020. https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/

EU Science Hub: The European Commission’s science and knowledge service. “Critical Infrastructure Protection.” Last modified 27 August 2019. Accessed 14 May 2020. https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

European Commission. “Cyber Security.” Last modified 7 July 2020. Accessed 7 July 2020. https://ec.europa.eu/digital-single-market/en/cyber-security

Geneva Internet Platform. Digital Watch Observatory. “UN GGE and OEWG.” Accessed 16 April 2020. https://dig.watch/processes/un-gge#view-7541-3

Greppi, Edoardo. “International Humanitarian Law in Cyber Operations.” ISPI Online. Published 2 May 2018. Accessed 20 November 2019. https://www.ispionline.it/it/pubblicazione/international-humanitarian-law-cyber-operations-20372

ICRC. Advisory Service on International Humanitarian Law. “What is International Humanitarian Law?” Published July 2004. Accessed 22 September 2020. https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf

ICRC. “Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Commentary of 2016. Article 2: Application of the Convention.” Accessed 30 June 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518#_Toc452041592

ICRC. “Cyber warfare: IHL provides an additional layer of protection. Statement delivered by Véronique Christory, senior arms control adviser for the International Committee of the Red Cross to the “Open-ended working group on developments in the field of information and telecommunications in the context of international security. New York- 10 September 2019.” Published 10 September 2019. Accessed 13 May 2020. https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection

ICRC Law & Policy. “Cyber-Warfare”. How does Law protect in War?. Accessed 13 May 2020. https://casebook.icrc.org/highlight/cyber-warfare

Karin, Nimrod. “Cyberwar, International Law, and the Tallinn Manual: A Puzzle of Positive Law and the Prism of Norm-Entrepreneurship.” The Hebrew University of Jerusalem. Accessed 20 November 2020. https://csrcl.huji.ac.il/book/what-international-law-cyberwar

Markoff, John.“Before the Gunfire, Cyberattacks”. Published 12 August 2008. Accessed 26 June 2019. https://www.nytimes.com/2008/08/13/technology/13cyber.html

Paganini, Pierluigi. “The Rise of Cyber Weapons and Relative Impact on Cyberspace.” Infosec. Published 5 October 2012. Accessed 3 February 2020. https://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/#gref

Pecorella, Giulia. “The US and the Information and Telecommunications in the Context of International Security: Which implications for the ius ad bellum?”. International Law Blog. Published 25 April 2016. Accessed 24 December 2019. https://internationallaw.blog/2016/04/25/the-us-and-information-and-telecommunications-in-the-context-of-international-security-which-implications-for-the-ius-ad-bellum/

Rugge, Fabio. “Armed Conflicts in the Cyber Age.” ISPI Online. Published 3 May 2018. Accessed 20 November 2019. https://www.ispionline.it/it/pubblicazione/armed-conflicts-cyber-age-20389

Schmitt, Michael N. and Liis Viul. “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms.” Just Security. Published 30 June 2017. Accessed 11 February 2020. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

Ticehurst, Rupert. “The Martens Clause and the Laws of Armed Conflict.” International Review of the Red Cross, No. 317. Published 30 April 1997. Accessed 18 January 2020. https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm

“What Are the Most Common Cyber Attacks?”. CISCO. Accessed 18 January 2020. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html