American University National Security Law Brief

Volume 5 | Issue 1 Article 4

2014

Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare

Ido Kilovaty

CYBER WARFARE AND THE *JUS AD BELLUM* CHALLENGES: EVALUATION IN LIGHT OF THE *TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE*

IDO KILOVATY[1]

1. INTRODUCTION

In 2010, the computer networks of the Iranian nuclear research facility in Natanz were infected by a malware, which caused unexpected detrimental physical destruction. The "Stuxnet" virus was specifically programmed to cause damage to the uranium-enriching infrastructure at the Natanz nuclear facility, achieving its goal in two different ways. Firstly, when specific configurations are met at the recipient network systems, Stuxnet forces the centrifuges to speed up to a speed that essentially destroys those centrifuges. Secondly, Stuxnet sends false signals to the monitoring system of the nuclear facility, obscuring real-time data and by doing so, thus disabling the safety system responsible for shutting down the facility in case such irregularities occur.[2]

In fact, Stuxnet managed to disrupt the process of uranium enrichment, causing devastating and irreversible damage to at least a thousand centrifuges out of a total of five thousand centrifuges in Natanz.[3] Today, it is believed that both the United States and Israel are behind the cyber attack on the Natanz nuclear facility, and that the Stuxnet virus had been intentionally designed to target and infect specifically configured network systems, namely those at the Natanz nuclear facility.[4] However, it was claimed that Stuxnet diffused and infected a Russian nuclear plant, as well as the International Space Station,[5] and more than just the Natanz nuclear plant computers were infected.[6]

The consequences of the Stuxnet virus were quite unprecedented. Unlike the preceding high-scale cyber attacks on Estonia in 2007, which targeted banks, telecommunication and other websites

---

1 LL.B. (Hebrew University of Jerusalem, '12), LL.M. (University of California, Berkeley, '14), S.J.D Candidate (Georgetown University, '17).

2 *See* William J. Broad, John Markoff & David E. Singer, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, THE NEW YORK TIMES (Jan. 15, 2011), *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=2&_r=0.

3 *See* Christopher Williams, *Barack Obama 'Ordered Stuxnet Cyber Attack on Iran'*, THE TELEGRAPH (June 1, 2012), *available at* http://www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-Stuxnet-cyber-attack-on-Iran.html.

4 *See* George Putic, *Suxnet: An Effective Cyberwar Weapon*, VOICE OF AMERICA (June 28, 2013), *available at* http://www.voanews.com/content/stuxnet-an-effective-cyberwar-weapon/1691311.html.

5 Sara Miller, *Stuxnet Has Infected Russian Nuclear Plant and International Space Station*, THE JERUSALEM POST (Nov. 12, 2013), *available at* http://www.jpost.com/International/Stuxnet-has-infected-Russian-nuclear-plant-and-International-Space-Station-331476.

6 Mark Clayton, *Stuxnet Cyberweapon Set to Stop Operating*, THE CHRISTIAN SCIENCE MONITOR (June 23, 2012), http://www.csmonitor.com/USA/2012/0623/Stuxnet-cyberweapon-set-to-stop-operating.

and databases while causing no physical destruction or loss of lives,[7] and the Russian cyber attacks during the 2008 War in Georgia, which were similar in their scale to the cyber attacks on Estonia,[8] Stuxnet was carried out by state actors, affecting and damaging physical infrastructure of another state. Such an operation can be characterized as an intervention, which is prohibited under the customary principle of non-intervention.[9] The same concept applies to the use of force or even an armed attack, which invokes the right to self-defense of Article 51 of the UN Charter. In that regard, some experts claim that the cyber attack on the Natanz nuclear facility was in fact an armed attack against Iran, triggering Iran's right for self-defense.[10] On the contrary, and arguably, the cyber attack on Natanz could be justified by anticipatory self-defense against an imminent threat.[11]

The example of the Stuxnet cyber attack illustrates the emerging cyber threats to the national security, following the constantly increasing capabilities of cyber attacks. Cyber attacks today and in the future are far from mere nuisance, and the capability of catastrophic destruction following a cyber attack is not a fantasy anymore.

There are numerous legal definitions to 'cyber attack' and 'cyber warfare'. One definition which might give a hint with regard to the scope of this thesis is the definition in the Tallinn Manual on the International Law Applicable to Cyber Warfare, which defines cyber attack as "[a] cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[12] This definition excludes cyber operations which do not, or are not expected to cause injury, death, or destruction. Those cyber operations are generally outside the analysis of *jus ad bellum*, since they do not reach the required severity that is usually associated with the use of force.

The novelty and unique characteristics of cyber warfare—also referred to as 'information warfare' by some scholars[13]—pose many challenges not only to the jus ad bellum but also to different branches of international law, such as the international humanitarian law, the international criminal law, and the intellectual property law. Some challenges include the following factors: who would qualify as a combatant in the cyber context, what measures an attacked state can employ to repel a cyber attack, and how the international law normally treats cyber espionage and the theft of intellectual property. Unfortunately, there is no consensus to those and other questions arising from the uniqueness of cyber warfare.

---

7 Heather Harrison Dinniss, Cyber Warfare And The Laws Of War 2 (2012).

8 Eneken Tikk et al., *Attacks Against George: Legal Lessons Identified*, Cooperative Cyber Defence Centre of Excellence, (Nov. 2008), http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

9 *See Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v. United States of America*), Judgment I.C.J. 1986, 14, ¶205.

10 *See, e.g.* Int'l Grp. of Experts, Tallin Manual on the International Law Applicable to Cyber Warfare §13 (Michael Schmitt ed., Cambridge University Press 2013) ("[A] closer case is the 2010 Stuxent operations. In light of the damage they caused to Iranian centrifuges, some members of the International Group of Experts were of the view that the operations had reached the armed attack threshold (unless justifiable on the basis of anticipatory self-defence (Rule 15)).").

11 *See id.* at §15.

12 *Id.* at §30.

13 *See, e.g.* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. Int'l L. & Pol. 57 (2001).

In chapter two, the uniqueness that is associated with cyber warfare will be reviewed in depth. This chapter will focus on the way in which this type of warfare differs from the common warfare, as it was known up till today. Moreover, discussing the uniqueness of cyber warfare will significantly simplify the understanding of how cyber warfare specifically challenges the *jus ad bellum*, which will be discussed later in this thesis.

In chapter three, the foundations of this thesis will be laid down by explaining and narrowing the research question of this thesis, namely how cyber warfare challenges concepts and principles of contemporary *jus ad bellum*. To clarify the scope of this thesis, the different international law fields that are interrelated and often associated with the *jus ad bellum* will be carefully mapped by briefly addressing questions of other international law branches with regard to the cyber attacks that are not part of the research in this thesis. In subsequent subchapters, the terminology that is typically used in the works of scholarship and official documents will be discussed and explained. In addition, more elaboration on the governing principles of the *jus ad bellum* will be given, in order to put cyber warfare in context, later in this thesis. This chapter will also introduce the most substantive piece of work on cyber warfare and applicable international law, the *Tallinn Manual*, as a means to engage with it later in the analysis.

In chapter four and its subchapters, the substantial analysis part of the research question will be extensively studied. This chapter will consist of naming the challenges that cyber warfare poses to the contemporary *jus ad bellum*. The chapter will also thoroughly analyze those cyber operations that amount to the use of force and even armed attacks, in order to establish a framework in which cyber operations become cyber warfare. Following that, significant challenges will be elaborated, such as the answers that the international law has (or does not have), the scholarly response to those challenges, and how it could affect the future in which cyber warfare is routinely employed. This chapter will also focus on the permissible measures that the attacked states can employ against cyber attacks.

After finalizing the substantial discussion in chapter three, chapter four will suggest some operative solutions to overcome some of the challenges that the cyber warfare poses to the jus ad bellum. This chapter will offer some atypical perspectives on some of the issues that this thesis raises, as well as discuss some of the prevalent criticism toward the policy making and governing of cyber warfare within the current international legal borders.

In chapter five, the research will be concluded with a suggestion of a number of possible solutions to the challenges discussed in this thesis. This chapter will also contain some insights as to where cyber warfare is currently going, and whether the international legal norms governing the right to resort to force are likely to catch up with the rapid development of this new technology that completely changes and re-defines the battlefield.

2. CHARACTERIZATION OF THE CYBERSPACE BATTLEFIELD

Nowadays, cyberspace has some unique characteristics that distinguish it from the traditional, physical, kinetic battlefield. Understanding those characteristics is moving one step forward toward identifying the challenges that cyber warfare poses to the jus ad bellum because those characteristics

are nonexistent in the world of the kinetic warfare.

2.1. National Dependency and Interconnectedness

Given the technological advantages, the tendency of states today to use electronic networks to base their 'critical infrastructure' is rapidly growing. This infrastructure generally consists of vital services, such as telecommunication, finance, transportation, energy and more.[14] Markets and governments depend greatly on those critical information infrastructures, and it is undisputed that nations today cannot function without those infrastructures.[15] The sensitivity of critical infrastructure could cause enormous damage when systems are disrupted, as well as affect networks of other sectors indirectly.[16] More importantly, the military highly depends upon electronic networks, mainly for communication and logistics.[17] Moreover, today cyber infrastructure is globally and domestically interconnected, which in turn prevents the distinction between the military and civilian infrastructure, making it difficult to isolate a specific cyber target, and subsequently causing uncertainty as to the scope of the damage that will be the result of the cyber attack eventually.

2.2. Anonymity

One of the factors that characterizes cyberspace is the anonymity of its users. Not only is cyberspace usually used anonymously, it is also possible for perpetrators to evade identification by sophisticated manners, such as proxy,[18] which masks the identity of the actual perpetrator, or simply by using computer in another uninvolved state, which causes confusion and false perpetrator identification by the victim state. Physical evidence, visibility and the intent of the perpetrator are all elements of anonymity, which differentiate the cyberspace battlefield from the physical one. Firstly, physical evidence exists in the physical battlefield, by means of the kinetic weapon used, the physical damage caused by that weapon, the intelligence that binds a specific perpetrator to the event, and more. However, in the cyberspace, there is a far lower to nonexistent amount of physical evidence and, at times, gathering such evidence is extremely challenging. Secondly, the intent and motivation are usually apparent from the investigation of a physical kinetic incident, while a cyber attack remains in most cases 'silent' with regard to the intent.

2.3. Simplicity, Quickness and Ease of Entry

Unlike war in the physical realm, cyberspace allows actions to be taken in fairly simple and quick ways. While physical actions require physical preparations, including troops, weaponry and

14 *See* Georg Kerschischnig, Cyberthreats and International Law 7 (2012).

15 *See* Branscomb Lewis and Mayer-Schonberger Viktor (eds.), *Protecting Our Future - Shaping Public-Private Cooperation to Secure Critical Information Infrastructures*, Report of a Roundtable of Experts and Policy Makers, 5 (May, 2006), *available at* http://www.vmsweb.net/attachments/pdf/Protecting-Report.pdf.

16 *See* Kerschischnig, *supra* note 14.

17 *See id.* at 8.

18 *See id.* at 9.

a precise military plan, cyber attacks—apart from preparing the specific plan or malware—only require, at their most unsophisticated form, a click of a mouse. Physical actions are also limited by their swiftness to a certain degree. For example, State A sends fighter jets to attack; State A is still bound by the fighter jets' speed limit and physical capabilities. On the other hand, cyber attacks can happen instantaneously, despite the geographical distance. Those factors are shaping a new system of conducting war, allowing the weak states that were unable to afford enormous military expenses to engage in a relatively cheap, simple and quick scheme for waging a war.[19] Moreover, the relative ease of entry brings a diversity of players. While the core idea of sovereignty is that states have the exclusive right to exercise power, cyberspace remains a realm that no entity exclusively owns. This difference demonstrates that states are not the only players anymore, and that the cyberspace includes non-state actors as well.

The high dependency of governmental infrastructures in cyberspace, the anonymity that the cyberspace encompasses, and the simplicity of the cyberspace altogether reflect the uniqueness of cyberspace as opposed to the traditional instruments of warfare. The research question and the necessary terms that are prevalent in this area of international law are then further examined.

3. DEFINING THE RESEARCH QUESTION, TERMINOLOGY, *JUS AD BELLUM* AND THE *TALLINN MANUAL*

Cyber operations in inter-state relations raise many difficult questions in different branches of international law. There is an extensive scholarship dealing with many of those questions, including how cyber warfare challenges the norms of the *jus in bello*, theft of intellectual property, cyber crimes, cyber espionage, and several others. However, all these challenging questions are not part of the research in this thesis, although many of the principles used to justify a solution to that challenge or another also apply to the challenges of the *jus ad bellum*. The primary issue that this thesis intends to thoroughly analyze and evaluate is the way cyber warfare—defined in subsequent chapters—challenges the contemporary rules that govern the use of force, namely *jus ad bellum*, and how the *Tallinn Manual* helps or complicates the reconciliation of those challenges.

The presumption of this thesis is that at the time that customary international norms governing the use of force were crystallized, and when the UN Charter was drafted following the Second World War, the Internet did not exist, and obviously cyber warfare was not accounted for.[20] There is an ongoing debate among scholars as to whether cyber warfare is fundamentally distinct from the traditional one, for the purposes of the applicability of the international law on cyber warfare, and whether the difference between the two would call for a new legal framework or the existing international law would then suffice, in case such a distinction existed.[21] Prominent scholars are using different considerations to establish their arguments, from pure legal considerations (relating to existing international law norms) to strategic considerations, which take into account some of the distinct characteristics of cyber warfare. Needless to mention, the range of arguments and

19 *See* Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 842 (2012).

20 *See* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B. C. INT'L & COMP. L. REV. 439, 454 (2009).

21 *See, e.g.* DINNISS, *supra* note 7, at 28.

conclusions is relatively diverse, as far as cyber warfare is concerned. However, it is quite undisputed that some general principles of the *jus ad bellum* and the law of armed conflicts are applicable to cyber warfare, yet even the supporters of the view that current rules and general principles are capable of regulating cyber warfare agree that there are normative gaps in the currently governing rules of an armed conflict.[22]

The purpose of this thesis is to analyze both the contemporary governing rules regulating the use of force and their possible applicability to cyber warfare–*lex lata*-and the optimal rules that could fill the gaps and eliminate the gross challenges that the governing rules pose to the concept of cyber warfare—*lex ferenda*.

In order for the research question to be successfully analyzed and answered in this thesis, the methodology employed would be summed up in the following points: (1) laying down the definition of the fundamental terms used in the cyber warfare scholarship, as well as determining the specific characteristics of cyber attacks, which distinguish it from the traditional kinetic warfare; (2) analyzing the norms of the contemporary *jus ad bellum* in general; (3) locating the challenges that cyber warfare poses to the norms of the *jus ad bellum* and evaluating those in the light of the provisions set forth in the *Tallinn Manual*; (4) combining the concept of cyber warfare with the norms of the contemporary *jus ad bellum*, analyzing cyber warfare in the light of the prohibition on the use of force, as well as its exceptions and discussing the challenges from different scholarly perspectives; (5) proposing viable solutions and interpretations of international law to deal with cyber warfare; and (6) concluding that which has been answered, and that which has been left undetermined, for more research in the future, by state practice or a further establishment of legal frameworks.

3.1. The *Tallinn Manual*

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (hereinafter the '*Tallinn Manual*') provides the international law—primarily the *jus ad bellum* and the *jus in bello*—applicable to cyber warfare. The *Tallinn Manual* is an initiative of the North Atlantic Treaty Organization (hereinafter 'NATO') Cooperative Cyber Defense Centre of Excellence, based in Tallinn, Estonia. The *Tallinn Manual* was published in 2012, and it is a non-binding set of rules, which was unanimously agreed upon by the group of experts assigned to draft the *Tallinn Manual*.

The *Tallinn Manual* consists of black-letter rules and a commentary for each rule presented. The rules reflect—according to the Manual—*lex lata* and not *lex ferenda*. Each rule reflects the consensus among the Group of Experts. Each rule is followed by a commentary that explains the legal basis of the rule, its practical implications, and necessary clarifications of the rule. Some commentaries also reflect the disagreement among the Experts. The Group of Experts consists of both academics and practitioners in the *jus ad bellum* and the *jus in bello* from different NATO member states. Some of the most reputable and authoritative experts in the *Tallinn Manual* are Prof. Michael Schmitt, Prof. Eric Jensen, and others. The work of the Experts drafting the *Tallinn Manual* was observed by the Allied Command Transformation, US Cyber Command and the International Committee of the Red Cross. The draft of the *Tallinn Manual* was peer-reviewed by other thirteen independent international

22 *See id.*

law experts.

The location in which the *Tallinn Manual* was drafted is not coincidental. In 2007, Estonia was a victim of a series of cyber attacks. The nature of the attacks being inter-state—rather than intra-state—spurred the legal debate on the international law that governs those inter-state cyber attacks. A dispute over the removal of a war memorial in Estonia triggered the cyber attacks against the country, which were at the time traced to Russia, although the latter refuted such claims.

The methodology employed in the *Tallinn Manual* was to apply and interpret existing international law, rather than create a specific new international law to regulate cyber warfare. Many provisions of the *Tallinn Manual* are based on the existing customary international law, treaties and judgments. However, even with regard to some existing fundamental customary international law norms, certain experts were ambivalent, as to whether those apply to cyber warfare at all.

The provisions in the *Tallinn Manual* can be divided into three main categories. First category rules are an explicit and direct application of international treaty or customary law (e.g., Rule 13 provides for self-defense against an armed attack). Second category rules are an elaboration of existing international law (e.g., Rule 11 provides the definition of use of force by offering a scholarly view of the definition). The third category of rules is the smallest, but it is worth mentioning nevertheless, and lists the rules that do not have an explicit origin in international law (e.g., Rule 7 poses an evidentiary burden, but is not claimed to have an origin in an international law norm). The classification into categories demonstrates the difficulty in accepting all of the rules provided by the *Tallinn Manual*; therefore, a close individual examination and analysis is required.

Many challenges arise in many of the *Tallinn Manual* rules, in some rules more than others. The scope of this thesis is to evaluate the main challenges of the *jus ad bellum* in cyber warfare, in the light of the *Tallinn Manual*'s provisions dealing with the *jus ad bellum*.

3.2. DEFINING AND DISTINGUISHING TERMINOLOGY

The extensive and diverse research, with regard to cyber warfare has generated countless terms to precisely articulate different actions used in the cyberspace. Some of those researches did not manage to accurately distinguish between one form and another of cyber action. Many of the researchers did not deem the terminology sacred in their writings. In order for this thesis to accurately differentiate between the various concepts and natures of cyber actions, this chapter will try to define the prevalent terminology in the cyber warfare research field.

3.2.1. COMPUTER NETWORK ATTACK (CNA)

Computer network attacks are "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[23] Computer network attack captures a wide range of hostile

23 U.S. Dep't of Def., *Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Nov. 8 2010) (as amended through 31 January 2011).

actions with the use of a computer code.[24] When the definition of the CNA is closely examined, it is revealed that this definition—despite capturing both—does not distinguish between a politically motivated CNA and non-politically motivated one. For the purposes of analyzing cyber warfare, the politically motivated CNAs are the ones of the most significance. Although NATO approved the definition set forth by the U.S. Department of Defense, it added, "A computer network attack is a type of cyber attack."[25] Interestingly, the NATO's *Glossary of Terms* does not define "cyber attack," but it could be that the NATO's purpose of adding that a CNA is a type of cyber attack was to include a political purpose in the definition of CNA. This will be further discussed in this chapter, in the definition of "cyber attack".

3.2.2. Cyber Crime

Cyber crime is understood as committing a crime with the use of a computer.[26] Unlike other terms, cyber crime lacks a generally accepted definition: "[T]here is still no accepted definition of what really constitutes cybercrime."[27] For the purposes of this thesis, cyber crime would involve the usage of a computer by non-state actors and in violation of criminal law.[28] Therefore, it seems that cyber crime is not part of the terminology in the subject of this thesis, as it fails to capture the potential violations of the international law governing the use of force.

3.2.3. Cyber Attack

Cyber attack is defined by the *Tallinn Manual* in rule 30 (*supra* page 7).[29] This definition of a cyber attack also seems to be adopted by the International Committee of the Red Cross (hereinafter: ICRC).[30] In addition, some scholars have made an effort to come up with their own unique definitions.[31] Yet, cyber attack appears to be a more suitable term for the analysis of the *jus ad bellum* and cyber warfare.

3.2.4. Cyber Warfare

Cyber warfare is not defined in the *Tallinn Manual*, despite being regularly used throughout the Manual. With regard to the definition, the Manual mentions, "[T]he term 'cyber warfare' is used here in a purely descriptive, non-normative sense."[32] The definition of the term is also absent

24 *See* Dinniss, *supra* note 7, at 5.

25 N. Atl. Treaty Org. [NATO], *NATO Glossary of Terms and Definitions*, at 2-C-12 (AAP-6) (2010).

26 *The Law of Cyber-Attack*, *supra* note 19, at 18.

27 Sylvia Mecado Kierkegaard, *International Cybercrime Convention*, in Cyber Warfare and Cyber Terrorism 469, (IGI Global 2008), *available at* http://www.igi-global.com/viewtitlesample.aspx?id=7486.

28 *The Law of Cyber-Attack*, *supra* note 19, at 18.

29 *Tallin Manual*, *supra* note 10, at §30.

30 Int'l Comm. of the Red Cross, *What Limits Does the Law of War Impose on Cyber Attacks?* (June 2013), https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

31 *See, e.g. The Law of Cyber-Attack*, *supra* note 19, at 10.

32 *Tallin Manual*, *supra* note 10, at 4, n. 17.

from the glossary.[33] The Joint Chiefs of Staff in the Joint Terminology for Cyberspace Operations defined cyber warfare as: "An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense and cyber enabling actions."[34]

It seems that contrasting cyber attack from cyber warfare would be equivalent to contrasting the use of force or an armed attack from war, while international law does not propose a binding definition of the term 'war.'[35] The definition of cyber attack and cyber warfare differ in the fact that cyber attack focuses on the gravity, amounting presumably to the use of force or an armed attack, while cyber warfare is a more general term, which focuses on the instrumental nature of such a war, and is used to define the conduct of war by the usage of cyber means, either wholly or partially. One definition of cyber warfare is "actions taken by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[36]

3.2.5. CYBERSPACE OPERATIONS

Cyberspace operations—also known as Cyber operations—are defined by the *Tallinn Manual* as "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."[37] The Joint Terminology for Cyberspace Operations used a similar definition.[38]

For purposes of uniformity throughout this thesis, the term 'cyber attack' will be used to address a single incident in the cyberspace with effects that arguably amount to the use of force or an armed attack. The term 'cyber warfare' will be used to address the general concept of the conduct of war with the means of cyberspace. The remainder of terms defined in this chapter will be used in citations and when a nuanced term is required for a better understanding of a specific concept.

The contemporary *jus ad bellum* will be discussed in the following chapter, in order to understand the legal framework that cyber warfare might be operating in.

3.3. THE CONTEMPORARY NORMS OF JUS AD BELLUM

3.3.1. PROHIBITION ON THE USE OF FORCE AND SELF-DEFENSE

Jus ad bellum—latin for "the right for war"—is the set of international law norms, which determines the time when it is lawful for states to resort to force.[39] Historically, the international law on the use of force has been constantly changing throughout the years, from the use of force that

33 *Id.* at 258.

34 DEP'T OF DEF., JOINT CHIEFS OF STAFF, JOINT TERMINOLOGY FOR CYBERSPACE OPERATIONS, *available at* http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

35 *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 4 (5th ed., 2011).

36 RICHARD CLARKE, ROBERT KNAKE, CYBER WAR – THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010).

37 *Tallinn Manual*, *supra* note 10, at 258.

38 *See* JOINT TERMINOLOGY FOR CYBERSPACE OPERATIONS, *supra* note 34, at §16.

39 *See* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. (forthcoming) 9 (2014).

required "just cause" in order to be permissible (*jus bellum iustum*), to use of force that was always permissible, and eventually to the unsuccessful attempt of absolute ban on war in the Covenant of the League of Nations and the Kellog-Briand Pact. As of today, the *jus ad bellum* is addressed in the UN Charter and by some customary international law principles. It primarily consists of a general prohibition on the threat or the use of force, embodied in Article 2(4) of the UN Charter: "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."[40]

According to the International Court of Justice in the *Nicaragua* judgment, the prohibition on the use of force is part of the customary international law.[41] Evidence to the prohibition on the use of force being part of customary international law can also be found in the Declaration on the Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (hereinafter: 'Friendly Relations Declaration'), which reaffirmed the duty of states to refrain from using or threatening to use force in their international relations.[42] The UN Charter contains two exceptions to the general prohibition on the use of force, being Security Council authorization to enact forcible measures as part of Article 42 and self-defense as prescribed in Article 51:

> [N]othing in the present Charter shall impair the inherent right of individual and 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.[43]

Interpreting some of the key terms ingrained in both the general prohibition on the use of force and the exception self-defense is complex. The Charter does not provide a definition of the term 'force'—neither did the International Court of Justice or the General Assembly.[44] The term 'armed attack' is characterized by the same ambiguity, although the International Court of Justice had—to some extent—addressed the term, as will be discussed below. The interpretational measures are explained in Article 31 and 32 in the Vienna Convention on the Law of Treaties (hereinafter:

40 U.N. Charter art. 2, para. 4.

41 *See Nicaragua*, 1986 I.C.J. at ¶ 188-90.

42 *Declaration on the Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations* (Declaration), G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).

43 U.N. Charter art. 51.

44 *See* Dinniss, *supra* note 7, at 40.

VCLT), which prescribed, *inter alia*, interpretational methods with regard to treaties.[45] Article 31(1) posits, "[A] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[46] Most experts agree that interpreting the terms "force" and "armed attack" in their ordinary meanings can be challenging, and point to the Charter's preamble and the Purposes of the United Nations in order to identify the "context."[47] One of those purposes, as mentioned in the preamble, is to ensure "that armed force shall not be used, save in the common interest."[48] Article 1 adds that the purpose of the United Nations is, among others, to "maintain international peace and security."[49] It appears that the preamble of the Charter establishes a goal to prevent the use of the armed force in inter-state relations. However, the general prohibition in Article 2(4) of the Charter does not indicate that the prohibition is on the "armed" force.[50] In case the interpretation employed with accordance to Article 31 of the VCLT leaves an ambiguous or obscure meaning, Article 32 to the VCLT establishes the resort to supplementary means of interpretation, namely "preparatory work of the treaty", better known as "*travaux préparatoires*".[51] At the time of the drafting of the Charter, the proposal of the Brazilian delegation to include economic coercion, within the general prohibition of Article 2(4), was rejected by a majority vote of 26 against 2.[52] It is therefore widely believed that the scope of the prohibition on the use of force covers the armed force, and excludes the political or economic coercion.[53] According to the analysis *supra*, escalation in diplomatic relations, the worsening of trade policies, sanctions and boycotts are not *per se* prohibited by Article 2(4) to the Charter,[54] unless they are carried out by the use of force.[55]

The prohibition on the use of force mentions that the prohibited use of force would be one that is "against the territorial integrity and political independence of any state." A restrictive reading of Article 2(4) would allow the use of force, which is neither against territorial integrity nor political independence, e.g. humanitarian intervention.[56] However, the prevailing perspective on the scope of the prohibition is that it also prohibits the use of force that is "in any other manner inconsistent with the Purposes of the United Nations." As mentioned before, one of the purposes of the United Nations is to maintain peace and security and encourage pacific resolutions of disputes.[57] Therefore, the prohibition on the use of force as set forth in Article 2(4) to the

45 Vienna Convention on the Law of Treaties §31-32, Jan. 27, 1980, 1155 U.N.T.S. 331 [hereinafter "VCLT"].
46 *Id.* at §31(1).
47 *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 904 (1999) [hereinafter "*CNA and the Use of Force*"].
48 U.N. Charter preamble.
49 U.N. Charter art. 1., para. 1.
50 *See CNA and the Use of Force*, *supra* note 47, at 904.
51 VCLT, *supra* note 45, at §32
52 *See CNA and the Use of Force*, *supra* note 47, at 905.
53 *See id.* at 908.
54 *See* KERSCHISCHNIG, *supra* note 14, at 106.
55 *See* Paul Szasz, *The Law of Economic Sanctions*, 71 U.S. NAVAL C. INT'L L. STUD.: THE LAW OF ARMED CONFLICT INTO THE NEXT MILLENNIUM 455, 455-56 (1998).
56 *See* KERSCHISCHNIG, *supra* note 14, at 107.
57 *See id.* at 108.

Charter is interpreted broadly to cover all threats and uses of force (armed), unless the use of force is exercised with accordance to the exceptions to the general prohibition (i.e., Security Council authorization under Chapter VII, or as explained below, under the exception of self-defense).

Article 51 of the Charter recognizes the 'inherent right' of self-defense. Similarly to the prohibition on the use of force, the International Court of Justice has affirmed the customary nature of the right to self-defense.[58] Article 51 also requires that "an armed attack occurs against a Member of the United Nations" in order to trigger the right to self-defense. Similarly to the discussion on the vague meaning of 'force' within Article 2(4) of the Charter, the term 'armed attack' is in no way any easier to define.

In the *Nicaragua* case, the International Court of Justice made an attempt to characterize an 'armed attack,' stating, "[I]t will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[59] In the same case, the Court proceeded to establish the 'scale and effects' test that would distinguish an armed attack from a mere frontier incident, which is not an armed attack.[60] According to the prevalent perspective and the *Nicaragua* judgment, there is a gap between the 'use of force' and an 'armed attack.'[61] An 'armed attack' poses a higher severity threshold than the 'use of force,' while a less severe and grave incident that amounts to the 'use of force' and not reaching the 'armed attack' threshold does not trigger the right to self defense, in accordance with Article 51 of the Charter.[62] This view was confirmed in the International Court of Justice *Oil Platforms* case.[63] According to the *Institut de Droit International*, "an armed attack triggering the right to self-defence must be of a certain degree of gravity," and "[a]cts involving the use of force of lesser intensity may give rise to counter-measures in conformity with international law."[64]

Definitions of the terms 'force' and 'armed attack,' out of the cyber context, remain ambiguous. The meaning of those terms will be better understood when their applicability to cyber attacks will be examined in subsequent chapters.

Both the prohibition on the use of force and the right to self-defense were unanimously applied to cyber warfare in the *Tallinn Manual*. Rule 10 of the *Tallinn Manual* applies Article 2(4) of the UN

---

58 *See Nicaragua*, 1986 I.C.J. at ¶ 176.

59 *Id.* at ¶191.

60 *Id.* at ¶195.

61 *See* Dinstein, *supra* note 35, at 207

62 *See id.* at 209.

63 *See Case Concerning Oil Platforms* (*Islamic Republic of Iran v. U.S.*), Judgment, 2003 I.C.J. 161, ¶ 51 (Nov. 6), *available at* http://www.icj-cij.org/docket/files/90/9715.pdf.

64 Institut de Droit Int'l, *Tenth Commission: Present Problems of the Use of Armed Forces in International Law*, Res. 10A (Oct. 27, 2007), *available at* http://www.idi-iil.org/idiE/resolutionsE/2007_san_02_en.pdf. The ILC Draft Articles on State Responsibility of 2001 also acknowledge that in Article 22: "The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of part three." In addition, Article 49 of the Draft Articles provides that "[a]n injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two." Article 50(1)(a) reaffirm that "the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations.".

Charter, as is, to cyber warfare, and reads as follows: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[65] Similarly, Article 51 of the UN Charter is applied, as well in Rule 13.[66]

Although Article 51 does not explicitly say so, an armed attack is not the only condition that establishes the right to self-defense.[67] In order for a state to invoke the right to self-defense when 'an armed attack occurs' against it, there are several customary international law requirements that must be fulfilled with regard to self-defense.

3.3.2. NECESSITY AND PROPORTIONALITY

A state engaging in self-defense must ascertain that the use of force in response to an armed attack is necessary and proportionate to the original armed attack. The meaning of necessity is that the victim state must first weigh a resolution of the conflict by non-forcible measures, and if those are available in response to the armed attack.[68] Non-forcible measures may include diplomacy, law enforcement or sanctions. In other words, forcible self-defense should be practiced only as a last resort, when a pacific resolution of the conflict is unavailable, and thus the use of force in response to the armed attack is necessary.[69]

Once the self-defense response is deemed necessary, it must be shown that such forcible response is proportionate. The principle of proportionality governs both the *jus ad bellum* and the *jus in bello*.[70] In the *jus ad bellum* context, proportionality has a quantitative and functional meaning.[71] The quantitative aspect of proportionality requires that the scale and effect of the counter-force must be similar to the armed attack.[72] The functional aspect requires that the use of force in self-defense be proportional to the objective of repelling the armed attack.[73] It is important to note, however, that the proportionality requirement does not limit the method—whether kinetic or cyber—that a victim state employs to repel an armed attack, but rather its intensity (scale and effect).

Following the 1837 *Caroline* incident, Secretary of State Daniel Webster made the famous statement with regard to 'necessity', by claiming that a state engaging in self-defense must demonstrate "necessity of self-defence, instant, overwhelming, leaving no choice of means and no moment of deliberation."[74] With regard to proportionality, it was established that "since the act justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it."[75] The International Court of Justice reaffirmed in several cases that both necessity and

65 *Tallinn Manual*, *supra* note 10, at §10.
66 *See id.* at §13, 54-61.
67 *See* KERSCHISCHNIG, *supra* note 14, at 119.
68 *See* DINSTEIN, *supra* note 35, at 232.
69 *See id.*
70 *See id.* at 233.
71 *See* Sheng Li, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38 YALE J. INT'L L. 179, 208 (2013).
72 *See* KERSCHISCHNIG, *supra* note 14, at 117, 120.
73 *See When Does Internet Denial Trigger the Right of Armed Self-Defense?*, *supra* note 71, at 208.
74 R.Y. JENNINGS ET AL., OPPENHEIM'S INTERNATIONAL LAW 420 (9th ed., 1996)
75 R.Y. Jennings, *The Caroline and McLeod cases*, 32 AM. J. INT'L L. 82, 89 (1938).

proportionality are prerequisites to invoke the right to self-defense. In *Nicaragua*, the International Court of Justice mentioned that necessity and proportionality are not embodied within the language of Article 51, and nevertheless, "self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law."[76] The International Court of Justice repeated the same idea in the Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*,[77] the *Oil Platforms* case,[78] and the *Armed Activities* case.[79]

3.3.3. Immediacy

A state responding in self-defense must do so within a reasonable timeframe.[80] The requirement of immediacy does not imply that self-defense must take place the instant an armed attack occurs, or minutes after that.[81] Preparing the armed forces and executing the self-defense cannot usually be immediate.[82]

3.3.4. Anticipatory Self Defense - Imminence

Whether anticipatory self-defense (or preemptive self-defense) is permissible under international law is highly debatable.[83] While the majority of states hold the view that anticipatory self-defense is a prohibited use of force,[84] the U.S. *Operational Law Handbook* mentions that self-defense could be employed against "hostile intent."[85] The U.S. policy on anticipatory self-defense is frequently called the 'Bush Doctrine.'[86] Supporters of the right to anticipatory self-defense rely on the requirement of 'imminence' of the threat:[87]

> [W]here there is convincing evidence not merely of threats and potential danger but of an attack being actually mounted, then an armed attack may be said to have begun to occur though it has not passed the frontier… If… the attack becomes manifestly imminent then it would be a travesty of the purposes of the Charter to compel a defending State to allow its assailant to deliver the first and perhaps

76 *Nicaragua*, 1986 I.C.J. at ¶94.
77 *Legality of the Threat or Use of Nuclear Weapons*, *Advisory Opinion*, 1996 I.C.J. Reports 226, 245 (Jul. 8, 1996).
78 *Iran*, 2003 I.C.J. at 198.
79 *Armed Activities on the Territory of the Congo* (*Dem. Rep. Congo v. Uganda*), 2005 I.C.J. 136, 223 (Dec. 19, 2005).
80 Dinstein, *supra* note 35, at 262, 267.
81 *Id.*
82 Kerschischnig, *supra* note 14, at 117.
83 *See* Christine D. Gray, International Law and the Use of Force 160 (3rd ed., 2008).
84 *See id.*
85 United States Army, Judge Advocate General's Legal Center and School, Operational Law Handbook, 86 (2007).
86 Preemptive Action in Self-Defense: National Security Strategy, 2001 Digest §x, at 947.
87 Avra Constantinou, The Right of Self-Defense Under Customary International Law and Article 51 of the UN Charter 115 (2000).

fatal blow. [88]

First, the conditions to use anticipatory self-defense are that the potential attacker has the capability to conduct the attack, or be on the verge of acquiring the capability.[89] Second, the anticipatory self-defense must only be used as the window of opportunity closes.[90]

3.3.5. ATTRIBUTION

A state engaging in self-defense measures must first identify the state responsible for the armed attack.[91] The assumption of State responsibility international law is that a state can be held liable if the illegal acts or omission were conducted on behalf of the state by a state organ, or if the state instructed, gave directions or controlled the non-state entity.[92]

The International Court of Justice in the case of *Nicaragua* concluded that in order for a responsibility to be imputed upon a state, it must have 'effective control' over the perpetrators:

> United States participation… in the financing, organizing, training, supplying and equipping of the *contras*… is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the *contras* in the course of their military or paramilitary operations in Nicaragua… For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had *effective control* of the military or paramilitary operations in the course of which the alleged violations were committed. (Emphasis added).[93]

On the contrary, the International Criminal Tribunal for the former Yugoslavia reached a different test of attribution in the *Tadić* case.[94] The court in this case took the view that an 'overall control' of a state over an organization would satisfy the attribution requirement. The overall control test is broader in its scope and more permissive in its nature, as the court noted, "If it is under the overall control of a State, it must perforce engage the responsibility of that State for its activities, *whether or not each of them was specifically imposed, requested or directed by the State*."[95] However, in

88 Claude H.M. Waldock, *The Regulation of the Use of Force by Individual States in International Law*, 1952 II RECUEIL DES COURS 451, 496-98.

89 *See Quo Vadis*, *supra* note 39, at 14.

90 *See id.*

91 *See* Levi Grosswald, *Cyber Attack Attribution Matters under Article 51 of the U.N. Charter*, 35 BROOK. J. INT'L L. 1151, 1153 (2011).

92 *See When Does Internet Denial Trigger the Right of Armed Self-Defense?*, *supra* note 71, at 203.

93 *Nicaragua*, 1986 I.C.J. at ¶¶ 64-5, 115.

94 *See Prosecutor v. Tadić*, Case no. IT-94-1-A, ICTY Appeals Chamber, Judgment (Jul. 15, 1999).

95 *Id.* at 122.

2007, well after the *Nicaragua* and *Tadić* judgments were rendered, the International Court of Justice in the *Bosnia Genocide* case rejected the *Tadić* overall control test by saying that 'the "overall control" test is unsuitable because it stretches too far, almost to breaking point, the connection that must exist between the conduct of a State's organs and its international responsibility.[96] In this case, the International Court of Justice used the *Nicaragua* effective control to resolve the question of State responsibility.

Dinstein includes attribution as part of necessity.[97] Dinstein posits, "[I]t is incumbent on the State invoking self-defence to establish in a definite manner that an armed attack was launched by a particular country against which it is forcibly responding, and by no other State."[98]

Articles 8, 9, and 11 to the Draft Articles on Responsibility of States for Internationally Wrongful Acts are generally referred to as the authority on State responsibility attribution framework.[99] A hostile act conducted by a person or a group is attributable to a state when: (1) the person or the group is acting under the direction or control of that state; (2) the person or the group is exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances, such as to call for the exercise of those elements of authority; or (3) when the conduct is not attributable to a state with accordance to Articles 8 and 9, when the state acknowledges and adopts the conduct in question.

It appears from the draft articles that the *Tadić* overall control test was not incorporated in those three articles, and that the effective control test is the governing test to determine State responsibility.

3.3.6. Less Grave Forms of Cyber Operations

Cyber operations that cannot be classified as armed attacks or use of force are not part of the *jus ad bellum* paradigm. Such cyber operations may qualify as interventions violating the principle of non-intervention.[100] In *Nicaragua*, the International Court of Justice noted that intervention is prohibited if it is:

> …[b]earing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in

96 *See Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosn. & Herz. v. Serb. & Montenegro*), Judgment, 2007 I.C.J. 43, ¶ 406 (Feb. 26).

97 Dinstein, *supra* note 35, at 231.

98 *Id.*

99 Draft Articles on Responsibility of States for internationally wrongful acts (adopted by the International Law Commission at its fifty-third session) (2001), §8-9, 11.

100 *See Nicaragua*, 1986 I.C.J. at ¶¶ 108, 202.

> the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[101]

The principle was also recognized in the Friendly Relations Declaration[102] and in the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty.[103] The meaning of the principle of non-intervention to cyber operations is that when it is coercive, it is violating the prohibition of intervention. In order to violate the principle of non-intervention, a cyber attack must interfere with the right of states to freely conduct their internal and external affairs. The non-intervention principle is somewhat similar to the use of force prohibition. However, the non-intervention principle also encompasses acts of lesser gravity that do not reach the use of force threshold, and not all cyber operations would be coercive. For instance, cyber espionage does not coerce a state in its political, economic, social or cultural system's free choices.

3.3.6.1. COUNTERMEASURES

A possible response to an act of prohibited intervention (that does not reach the armed attack threshold) is countermeasures. Countermeasures are a form of unilateral, non-forcible self-help employed by an injured state in response to internationally wrongful acts by another state.[104] Countermeasures are illegal, unless they are employed in response to the wrongful act.[105] There are several limitation to the permissible countermeasures and the way in which they are allowed to be carried out, however, countermeasures in cyber warfare require a whole separate discussion and research. Needless to say that countermeasures are outside of the *jus ad bellum* analysis.

We move to the substantial discussion on the challenges of the *jus ad bellum* in the context of cyber warfare.

4. IDENTIFICATION OF THE TECHNICAL AND SUBSTANTIVE *JUS AD BELLUM* CHALLENGES OF CYBER WARFARE

After viewing the definitions, characteristics and the relevant contemporary *jus ad bellum*, it is time to proceed to the core of this thesis – namely, the challenges that cyber warfare poses to the

---

101 *Id.*

102 G.A. Res. 2625 (XXV), *supra* note 42.

103 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, G.A. Res. 2131 (XX) (Dec. 21, 1965).

104 Katharine Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 14 (2011); *see also* Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, in Rep. of the Int'l Law Comm'n, 53d sess., Apr. 23-June 1 & July 2-Aug. 10, 2001, pt. 3, ch. II, ¶¶ 1, 3, U.N. Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001), *available at* http://untreaty.un.org/ilc/publications/yearbooks/Ybkvolumes(e)/ILC_2001_v2_p2_e.pdf.

105 ILC Draft Articles, *supra* note 99, at §22.

jus ad bellum given its unique characteristics and vulnerabilities. Analyzing the challenges would be irrelevant if cyber attacks are unable to amount to the 'use of force' or 'armed attack'; therefore, the primary question is whether cyber attacks have the capability to reach the threshold of the 'use of force' or 'armed attack.'

4.1. International Law Ambiguity

Customary international norms have not developed, with regard to cyber warfare. Also, there is not any specific treaty (or making thereof) to govern cyber warfare.[106] There is ambiguity as to whether the current *jus ad bellum* applies, under what conditions the use of force invokes the right of self-defense, and how the right of self-defense is limited in cyberspace. The *Tallinn Manual* is a NATO initiated project to reflect the international law governing cyber warfare, according to the Group of Experts who drafted the rules in the *Manual*.[107] The Group of Experts was naturally chosen from the NATO member countries, most prominently from the United States, the United Kingdom, and Western Europe. Considering the identity of the experts and the possible perspective bias, it is questionable to what extent the *Tallinn Manual* represents an international perspective on the international law applicable to cyber warfare.

To illustrate this controversy, two separate governmental initiatives were undertaken by the United States and Russia-China to understand the scope of the international law applicable to cyber attacks.[108] Unsurprisingly, the two initiatives reached absolutely different conclusions.[109] While according to the United States a cyber attack is "a hostile act using computer . . . intended to disrupt . . . critical cyber systems,"[110] the Shanghai Cooperation Organization took a broader view, defining "information war" as an act of state to impair another state's "political, economic and social systems."[111] The two perspectives represent a core question, regarding the types of coercions covered by the use of force paradigm. There is an ongoing debate as to whether political and economic coercions are covered by the scope of the use of force paradigm. The *Tallinn Manual* explicitly notes that "whatever 'force' may be, it is not mere economic or political coercion."[112]

It is also important to note that the ambiguity is limited in its scope. For example, the view that international law applicable to cyber warfare should be created from zero is not very prevalent in the academic discourse. The White House Strategy for Cyberspace summarizes the primary challenge of cyber warfare, stating:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render

106 *See Tallinn Manual*, *supra* note 10, at 5.
107 *See id.*
108 *See The Law of Cyber-Attack*, *supra* note 19, at 824.
109 *See id.*
110 Joint Terminology for Cyberspace Operations, *supra* note 34, at §10.
111 Tom Gjelten, *Seeing the Internet As An 'Information Weapon'*, NPR (Sep. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.
112 *Tallinn Manual*, *supra* note 10, at 46.

> existing international norms obsolete Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace. [113]

The White House's statement is precise in delimiting the scope of this thesis. On one hand, some norms of international law apply to cyber warfare, without any specific difficulties. On the other hand, some points still require careful consideration and creation of *lex specialis* to deal with cyber warfare's distinctiveness. The EU Commission also shares this view; in its Internet Policy and Governance draft, it concludes that cyberspace is "subject to the same laws and norms that apply in other areas of our day-to-day lives."[114]

4.2. CYBER ATTACKS AS ARMED COERCION

Since the drafters of the UN Charter were not foreseeing that wars could be conducted in the cyberspace,[115] the question that appears to be highly arguable among scholars is the applicability of the *jus ad bellum*, as promulgated, *inter alia*, in Article 2(4) and 51 to the UN Charter on cyber attacks. Three approaches have been presented by scholars as to whether a cyber attack could constitute an armed attack, namely the instrument-based approach, the target-based approach, and the effects-based approach.[116]

4.2.1. THE INSTRUMENT-BASED APPROACH

As the name suggests, the instrument-based approach focuses on the coercive instrument used.[117] Traditionally, the paradigm of the use of force was based on the instrument-based approach.[118] In order for an attack to qualify as an armed attack, the weapon employed must be of a kinetic nature. Weapons that would qualify under this approach would be traditional weapons, such as conventional weapons, chemical weapons, biological weapons and nuclear ones. The instrument-

113 The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* 9 (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

114 *European Commission on Internet Policy and Governance*, *available at* http://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-72-EN-F1-1.Pdf.

115 *See When Does Internet Denial Trigger the Right of Armed Self-Defense?*, *supra* note 71, at 186.

116 *See* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 91 (2010).

117 *CNA and the Use of Force*, *supra* note 47, at 909.

118 *Id.*

based approach analyzes whether the destructive physical damage resulted from the kinetic force of the weapon used.[119] The advantage of the instrument-based approach is predictability, given the simplicity in which only the assessment as to whether a kinetic weapon has been used is required.[120]

Article 41 of the UN Charter provides further support to the notion the cyber attacks could not meet the 'armed attack' threshold. Article 41 reads, "[T]he Security Council may decide what measures *not involving the use of armed force* are to be employed to give effect to its decisions … These may include … telegraphic, radio, and other means of communication."[121] (Emphasis added).

Under this approach, diplomatic or economic coercions would be classified as interventions, while military coercion would satisfy the threshold of the use of force and armed attack.[122] Therefore, cyber attacks would seldom reach the threshold of military coercion, and hence, rarely constitute an "armed attack."[123] Most scholars today do not hold the view that the instrument-based approach applies to cyber attacks.[124] However, it is important to note that most scholars today reject the instrument-based approach, due to being "dangerously outdated."[125] Yet, this was the approach used since the promulgation of the UN Charter.[126]

4.2.2. The Target-based Approach

The target-based approach posits that any cyber attack against critical cyber infrastructure is an armed attack.[127] This approach disregards the gravity of the attack and focuses on the target of the cyber attack that would justify a forcible response by the victim state, namely a strict liability regime.[128] According to the target-based analysis, it is more likely for a military escalation to happen when a cyber attack occurs, given the fact that no kinetic effect is required in order to trigger the right to self-defense.[129]

Defining 'critical infrastructure' turns to be another complicated task. According to the UN General Assembly, "critical infrastructures" is described as: "…those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations."[130]

---

119 Michael Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, 4 Int'l Conference on Cyber Conflict 283, 287 (2012), *available at* http://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf.

120 *CNA and the Use of Force*, *supra* note 47, at 917.

121 U.N. Charter art. 41.

122 *CNA and the Use of Force*, *supra* note 47, at 909.

123 Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023, 1041 (2007).

124 *See The Law of Cyber-Attack*, *note* 19, at 846

125 *See id.*

126 *See CNA and the Use of Force*, *supra* note 47, at 909.

127 Walter Gary Sharp, Cyberspace and the Use of Force 129–30 (1999)

128 *See When Does Internet Denial Trigger the Right of Armed Self-Defense?*, *supra* note 71, at 186.

129 *See The Law of Cyber-Attack*, *note* 19, at 846-7.

130 Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, G.A.

The US Patriot Act also defines critical infrastructure as: "…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[131]

According to the target-based approach, any penetration to those critical infrastructures is an armed attack, triggering the right to self-defense. Neither the instrument (the cyber attack) nor the kinetic effect (death or injury) is part of the analysis of the target-based approach.

4.2.3. THE EFFECTS-BASED APPROACH

Since the instrument-based approach disqualifies many cyber attacks from reaching the armed attack threshold and the target-based approach is overbroad, a third approach used in the assessment of whether a cyber attack amounts to an armed one has emerged. The target-based approach—or the consequence-based approach—was articulated by Michael Schmitt in his renowned article on *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*.[132] The approach was developed in order to deal with the disadvantages of the instrument and target-based approaches. There are several arguments in support of the effects-based approach. Firstly, the potential lethal nature of cyber attacks should not be excluded solely on the grounds that the UN Charter drafters were not aware of the possibility of those attacks in the future.[133] Secondly, in abstract, law is intended, *inter alia*, to prevent certain outcomes. Therefore, a consequences-based approach is better suited to prevent severe cyber attacks.[134] Dinstein maintains, "[I]t does not matter what specific means - kinetic or electronic - are used to bring about, but the end result must be that violence occurs,"[135] and several other scholars also support the effects-based approach.[136]

The consequences of cyber attacks can range from a mere nuisance to physical damage and death, as well as negative economic and social effects.[137] The goal of the effects-based approach is to characterize a cyber attack on this continuum, and to distinguish between military coercion cyber attacks and the economic or political ones.[138] The criteria are as follows: (1) *Severity* - the degree of the physical destruction caused by the cyber attack. Armed coercion tends to cause greater physical damage. (2) *Immediacy* - the amount of time elapsed since the attack began and until the consequences emerged. Armed coercion is more likely to have immediate effects. (3) *Directness* - armed coercion usually causes physical damage that can be directly tied to the attack itself. (4) *Invasiveness* - the more intrusive the attack is, the higher the chances it is armed coercion.

Res. 58/199, U.N. Doc. A/RES/58/199 (Jan. 30, 2004).

131 42 U.S.C. 5195c(e).

132 *CNA and the Use of Force*, *supra* note 47.

133 *"Attack" as a Term of Art*, *supra* note 119, at 287.

134 *Id.*

135 DINSTEIN, *supra* note 35, at 88.

136 SHARP, *supra* note 127, at 88-93.

137 *CNA and the Use of Force*, *supra* note 47, at 912.

138 *See id.* at 914.

Intrusiveness is evaluated by the degree of which the target system is secured.[139] (5) *Measurability* – the effects caused by armed coercion can be easily measured, while the ones followed by economic or political coercions are harder to measure. (6) *Presumptive Legitimacy* - international law explicitly prohibits the use of (armed) force. If the nature of the attack is not per se prohibited by international law, it is therefore permitted, and vice versa.

Schmitt's six-criteria paradigm was incorporated wholly in the *Tallinn Manual*, as part of Rule 11, defining the use of force, which reads, "[R]ule 11 - Definition of use of force: 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."[140] The commentary that accompanies this rule mentions that Schmitt's criteria as a method for states "when deciding whether to characterize any operation, including a cyber operation, as a use of force," and that the criteria are "merely factors that influence States making use of force assessment . . . not formal legal criteria."[141] The language of the *Tallinn Manual* suggests that Schmitt's criteria apply to any use of force, regardless of whether a cyber attack was launched. Moreover, the *Tallinn Manual* includes two additional criteria to the paradigm: the military character and state involvement.[142] As of the military character, a nexus between the cyber attack in question and military operations makes it more likely for the attack to be qualified as a use of force incident, and as of state involvement, the more direct the participation of a state in the cyber attacks is, the more likely it is a use of force act.[143]

The criteria paradigm of the effects-based approach can potentially cause obscurity and unpredictability in assessing whether a cyber attack amounts to the use of force. Given the fact that the substantial state practice is currently unavailable, the analysis will lead to many gray area cases.[144] In addition, the *Tallinn Manual* claims only to apply existing international law. However, the 'Schmitt Criteria' is viewed by some as an attempt to prescribe a new law.[145]

The effects-based approach could also be supported by the International Court of Justice, Nicaragua case, where the court employed a broad interpretation of Article 2(4).[146] Moreover, the court in the advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons* concluded that the *jus ad bellum* applies to "any use of force, regardless of the weapons employed."[147] The view of the court in the *Nuclear Weapons* advisory opinion illustrates that the instrument-based approach is not necessarily the prevalent approach in assessing whether the *jus ad bellum* applies to a specific weapon. The court used the same approach with regard to the *jus in bello*.[148]

---

139 *Tallinn Manual*, *supra* note 10, at 49.

140 *Id.* at 45.

141 *Id.* at 48.

142 *Id.* at 50.

143 *See id.* at 50-51.

144 *See CNA and the Use of Force*, *supra* note 47, at 919.

145 *Tallinn Manual*, *supra* note 10, at §11, commentary 9 (Although the Tallinn Manual suggests that it applies law "as is," the criteria is viewed as an attempt to prescribe new law. One such argument is made by Lianne J.M. Boer, *'Restating the Law 'As It Is': On the Tallinn Manual and the Use of Force in Cyberspace*, 5:3 Amsterdam Law Forum 4, 6 (2013).).

146 *See Quo Vadis*, *supra* note 39, at 9.

147 *Nuclear Weapons*, *supra* note 76, at ¶39.

148 *Id.* at ¶78. The court talked about the "Martens Clause", which was at first presented in the preamble of Hague Convention II of 1899, and later used in Article 1(2) of the Additional Protocol to the Geneva Convention (Protocol I).

Moreover, Harold Koh, former legal adviser of the U.S. State Department, in his speech at the U.S. Cyber Command Inter-Agency Legal Conference on the applicability of international law to cyberspace, was asked whether 'cyber activities ever constitute a use of force.'[149] Koh responded positively: "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[150] However, while this is the view of the Department of State, it is important to understand that different states will not necessarily hold the same views. General Keith Alexander, a nominee[151] for the U.S. Cyber Command said:

> There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force. Thus, whether in the cyber or any other domain, there is always potential disagreement among nations concerning what may amount to a threat or use of force.[152]

Not only some states oppose the effects-based approach and its criteria, but also some scholars criticize the Schmitt Criteria on the grounds that it is over inclusive, as Silver notes:

> Examination of the criteria suggests that virtually any event of [computer network attack] can be argued to fall on the armed force side of the line, except perhaps as regards the criterion of severity, and that the criterion of severity in effect is just another way of articulating the observation that, for an event of [computer network attack] to be considered a type of force under Article 2(4), it must produce personal injury or property damage similar to that caused by military weapons.[153]

On a final note, while the *Tallinn Manual* intends to reflect the *lex lata*, rather than the *lex ferenda*, with regard to the international law applicable to cyber warfare; it is important to note that the

---

The purpose of the clause is to apply the *jus in bello* provisions and customs to cases not explicitly covered by the Geneva Conventions. The Martens Clause posits that 'principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience' to those cases. In the *Nuclear Weapons Advisory Opinion*, the ICJ affirmed that the Martens Clause 'proved to be an effective means of addressing the rapid evolution of military technology'.

149 Chris Borgen, *Harold Koh on International Law in Cyberspace*, OPINIO JURIS (Sep. 19, 2012), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace.

150 *Id.*

151 Keith Alexander was appointed by the U.S. Senate as Cyber Command commander on May 7, 2010. He served as commander from May 21, 2010 until March 28, 2014.

152 Duncan Hollis, *Reading Tea Leaves in Confirmation Hearings for U.S. Cyber Commander*, OPINIO JURIS (Mar. 18, 2014), http://opiniojuris.org/2014/03/18/reading-tea-leaves-confirmation-hearings-u-s-cyber-commander.

153 Daniel Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUDIES 73, 89 (2002).

'*Tallinn Manual*' does not consider itself a legally binding document.[154] Moreover, the effects-based approach criteria appear in the commentary part, which does not represent the *lex lata*, and the *Manual* explicitly states that the criteria are not legally binding.[155] It is unclear whether the criteria represent the contemporary *jus ad bellum*, given the fact that it is not part of any primary source of international law.[156] Therefore, we move forward to discuss the legal standing of the effects-based approach criteria.

4.2.3.1. The Legal Source of the Effects-based Approach

The effects-based approach is not provided by the UN Charter or any other international legal instrument. In the commentary to Rule 11 of the *Tallinn Manual* on the prohibition of use of force or threats, the *Manual* states:

> The approach suggests that States are likely to consider and place great weight on the following factors, inter alia, when deciding whether to characterize any operation, including a cyber operation, as a use of force. It must be emphasized that they are merely factors that influence States making use of force assessments they are not formal legal criteria.[157]

Schmitt himself admitted that the criteria were influenced by a policy-oriented approach.[158] The *Manual* does not intend to cite any international law sources in support of the criteria. It is clear that the criteria do not represent explicit international law, neither the treaty law nor the customary one. In addition, the *Manual* does not create new international law because it lacks the mandate to do so. The furthest the criteria can go is to represent the "teachings of the most highly qualified publicists of the various nations," as provided in Article 38 of the Statute of the International Court of Justice, which lists the sources of international law to be applied by the Court (and is believed to represent international law sources overall). However, those teachings can only serve as subsidiary means to clarify international law. Moreover, despite the fact that the *Tallinn Manual* has some of the most qualified and reputable experts, it does not have experts of *various* nations as suggested in Article 38 of the Statute. Therefore, the criteria are neither old nor new, in regard to law.

If the *Manual* informally creates the criteria—in contrast to creating international law—rather than basing it on existing law, this will raise the question of why exactly those specific criteria were chosen over others, and what the interaction of the different criteria among themselves is. Some scholars based the criteria on "intuition," and provided "[t]his raises the question of why states would follow these intuitions regarding the *factual* behavior of states when confronted with *normative*

154 *Quo Vadis*, *supra* note 39, at 2.
155 *Tallinn Manual*, *supra* note 10, at 48, commentary 9.
156 Article 38(1) of the Statute of the International Court of Justice.
157 *Tallinn Manual*, *supra* note 10, at 48, commentary 9.
158 *See* Michael Schmitt, *The "Use of Force" in Cyberspace: A Reply to Dr. Ziolkowski*, 4 Int'l Conference on Cyber Conflict Proceedings 311, 317 (2012).

questions regarding the scope of application of the prohibition on the use of force."[159] The criteria could also mean that the drafters of the *Tallinn Manual* expect states to develop customary international law along the lines of those criteria.[160]

It seems that the criteria are not entirely legal, but represent, to some extent, a political view. However, it seems inconsistent to employ political standards in assessing a legal situation. The use of force entails State responsibility, and using political standards to hold a state accountable seems contradictory to the purpose of international law and the law on State responsibility.

4.2.4. CYBER ATTACKS AS POLITICAL OR ECONOMIC COERCION

As discussed above, in order for a cyber attack to qualify as one involving the use of force, it must cause certain physical destruction or injury or death to persons, and as already mentioned, Brazil's proposal to include political and economic coercion in the scope of the use of force was rejected.[161] However, in the age of cyber warfare, economic and political coercion by the use of code or viruses could be even more destructive than a cyber attack with physical destruction. While conventional warfare focused on causing physical consequences, cyber warfare is expected to cause comparable damage with no physical consequences.[162] There is a possibility that this gap between traditional warfare and economic coercion will be exploited in order to avoid State responsibility for internationally illegal acts.[163] Cyber attacks effects range from "mere inconvenience to physical destruction and death . . . It can affect economic, social, mental and physical well-being, either directly or indirectly, and its potential scope grows almost daily, being capable of targeting everything from individual persons or objects to entire societies."[164] One example could be a cyber attack that shuts down the New York Stock Exchange for a week. While it causes no tangible or visible damage, it results in the loss of enormous amounts of money, due to the inactivity of the financial market, as well as collateral damage caused by such inactivity. Some will argue that even though this damage is not kinetic, i.e. was not caused by an explosive or physical destructive reaction; it is even more severe than a small physical damage or an injury of a single person. According to the view that the use of force may only be of an armed nature, a cyber attack on the New York Stock Exchange will not qualify as an act involving the use of force. Similarly, the cyber attacks on Estonia that shut down banking websites were not viewed as use of force incidents. Another comparison to illustrate the anomaly is a limited border incursion, which qualifies as the use of force under the current interpretation, and the 1973-1974 Arab Oil Embargo, which is both politically and economically coercive with consequences that exceed in their severity the consequences of the incursion.[165] Such an anomaly requires reconsidering the scope of the prohibition of the use of

159 Kessler and Werner, *Expertise, Uncertainty and International Law: A Study of the Tallinn Manual on Cyberwarfare*, 26(4) LEIDEN J. OF INT'L L. 793, 809 (2013).
160 *See id.*
161 *CNA and the Use of Force*, *supra* note 47, at 905.
162 *See Information Warfare and International Law on the Use of Force*, *supra* note 13, at 58.
163 *See id.*
164 *CNA and the Use of Force*, *supra* note 47, at 912.
165 *Id.* at 909.

force in the age of war in the fifth dimension.

An example of economic coercion could be found in the events of April 23, 2013. A group named Syrian Electronic Army hacked the Associated Press Twitter account. Following the successful operation, the group posted the following tweet on the Associated Press account: "[T]wo Explosions in the White House and Barack Obama is injured."[166] Immediately after the fake tweet was posted, and in a matter of only two minutes, the Dow Jones index plunged by about 145 points; equal to nearly 150 billion dollars.[167] Although the market recovered soon after the hoax was revealed, such cyber operation demonstrates the capability to cause major economic damage with no casualties or physical damage. The relative easiness in manipulating the public and causing subsequent economic damage requires rethinking the limits of what the use of force paradigm encompasses.

One view to reconcile this anomaly is to realize that international law content, interpretation and application change in accordance with the changing security environment and threats.[168] When states eventually understand that cyber attacks of an economic or political coercive nature are as severe as an armed use of force action, then the interpretation of the use of force scope will also include economic and political coercions. It is believed that a state will, in fact, treat data destruction as equivalent to physical destruction.[169] Even in the *Tallinn Manual* itself, some experts took the approach of severity of consequences—rather than physical effects—in order to determine the use of force.[170] It is also clear that this approach was adopted by some experts to include the targeting of a state's economic infrastructure within the scope of the use of force prohibition.[171]

The proposal suggested by the author is to include the gravest uses of political and economic coercions in the scope of the use of force paradigm. An example of a grave use of economic coercion is shutting down the entire credit card transactions clearance system, causing collateral damage and preventing transactions from being processed. Such a type of cyber attack, while not causing direct casualties or physical tangible damage, causes severe and serious damage affecting people's daily routines. The inclusion of political and economic coercions in the use of force paradigm is limited only to the most severe, grave and serious attacks with effects that are comparable to kinetic attacks. Needless to say that such a proposal should either have a basis in emerging state practice, or be specifically agreed upon in a cyber treaty. The inclusion of the gravest political and economic coercions will contribute to the purposes of the Charter, which are maintaining peace and minimizing the use of force between states. As of today, contemporary international law does not view political or economic coercions as a prohibited type of use of force.

Following the discussion on political and economic coercions as being use of force models, we

---

166 David Jackson, *AP Twitter feed hacked; no attack at White House*, USA Today (Apr. 23, 2013), available at http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/.

167 *See* Peter Foster, *'Bogus' AP tweet about explosion at the White House wipes billions off US markets*, The Telegraph (Apr. 23, 2013), *available at* http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

168 *See Quo Vadis*, *supra* note 39, at 3.

169 *See id.* at 11.

170 *See id.* at 11-2.

171 *See id.* at 12.

move to examine the challenge of attribution.

4.3. THE REQUIREMENT OF ATTRIBUTION

Attributing a cyber attack to a state can prove to be a challenging task. Cyber attackers are capable of denying tracing or blurring their identities, through the usage of several cyber techniques. The difficulty of identifying the perpetrator lies not only in the evasion techniques employed, but in the following characteristics. Firstly, the Internet does not have an effective "per-call" basis charge like telephone services; this affects the tracking and tracing of the Internet users.[172] Secondly, the Internet lacks the international cooperation framework between the jurisdictions involved in a cyber attack. While the International Telecommunications Union provides such a framework for the telephone system, such agreement does not currently exist between nations.[173] Thirdly, in the past, business did not actively support the investigation and attribution of a cyber attack. Businesses preferred to reboot their servers and resume in their affairs. As cyber attacks became more sophisticated and dangerous, the need for attribution and an adequate response grew almost instantaneously.[174] Those three challenges intensify the main problem of attribution—that is the techniques of the evasion of the perpetrator's identity. In their article *Techniques for Cyber Attacks Attribution*, David Wheeler and Gregory Larsen conclude:

> [A]ttribution is difficult and inherently limited. In particular, attackers can cause attacks to be delayed and perform their attacks through many intermediaries in many jurisdictions, making attribution difficult. In some cases this can be partly countered, for example, by treating some information-gathering techniques as attacks (and attributing them), using multiple techniques, and using techniques that resist this problem (such as exploiting/forcing attacker self-identification and attacker surveillance). Nevertheless, because of the difficulty and uncertainty in performing attribution, computer network defense should not depend on attribution. Instead, attribution should be part of a larger defense-in-depth strategy.[175]

The way in which some cyber attackers mask their identities is through a method called "Stepping Stones."[176] According to this method, a cyber attack is routed through third-party

---

172 Jeffrey Hunker et al., *Roles and Challenges for Sufficient Cyber-Attack Attribution*, INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION 5 (Jan. 2008), *available at* http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

173 *Id.* at 6.

174 *See id.*

175 David Wheeler et al., *Techniques for Cyber Attack Attribution*, INSTITUTE FOR DEFENSE ANALYSES 53 (Oct. 2003), *available at* http://handle.dtic.mil/100.2/ADA468859.

176 *Cyber Attack Attribution Matters*, *supra* note 90, at 1167.

computers, which usually belong to an uninvolved state.[177] For instance, Ruritania launches a cyber attack against Utopia, routing the attack through a computer system in Arcadia. When the cyber attack occurs in Utopia, Utopia tries to identify the perpetrator of the cyber attack, tracing it back to Arcadia, not realizing that Arcadia is an innocent state. However, even though cyber attackers can evade or delay their identifications, some techniques are still available to overcome the identification difficulty—seventeen of them being proposed by Wheeler's and Larsen's article.[178]

To refine the attribution challenge even better, it must be compared to traditional kinetic attacks. Cyber attacks differ from the kinetic world, in which attacks are conducted in the physical dimension.[179] Kinetic attacks tend to leave physical and circumstantial evidence, such as the identity of the soldiers or the weapons employed, the geographical location in which the attack occurred, witnesses and more, while the cyberspace dimension lacks those types of evidence.[180] This difference between cyber attacks and the kinetic ones strengthens the notion that the law of attribution is obsolete or stringent, in the context of attributing cyber attacks. Such a claim has yet to be examined by state practice and the specificity of the difficulty, rather than a potential challenge of an abstract nature.

Identifying the perpetrator is not sufficient to attribute the cyber attack to a state. Locating the attacker is only the first step out of three, in order to trigger the right to lawful self-defense. Following the process of identifying the attacker, the attacker and his action must be attributed to a specific state. The attribution tests are discussed above in chapter 3.3.5. After those two steps, the response should fulfill the requirements of necessity and proportionality, and as part of those requirements, it must also be immediate or it runs the risk of becoming an unlawful reprisal. In contrast to a kinetic armed attack, in the cyber context, the effects of a cyber attack are not always immediate. Moreover, the time-consuming attribution process might also interfere with the immediacy requirement. Therefore, the immediacy requirement is sometimes challenged in the cyber context.[181]

A victim state is also required to show "clear and compelling" evidence of state involvement in a cyber operation.[182] Since state actions are assessed by what was known to the state at the time of its action, the state is required to establish a reasonably compelling evidence, which would be more than the civil "more likely than not" standard, but lower than the criminal "beyond a reasonable doubt" standard.[183]

However, not all cyber attacks can be attributed to a state. We proceed to examine the problem of independent non-state actors as cyber attackers.

177 *Id.*
178 *See* Wheeler, *supra* note 175, at 9.
179 Grosswald, *supra* note 91, at 1166.
180 *See id.* at 1167.
181 Kerschischnig, *supra* note 14, at 137-139.
182 Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 Vill. L. Rev. 569, 595 (2011).
183 *Id.*

4.3.1 NON-STATE ACTORS IN CYBERSPACE

As already mentioned earlier in this thesis, some cyber attacks are carried out by independent non-state actors who are not affiliated to the state in any way, and as so, it is questionable whether a victim state can exercise its right to self-defense against non-state actors. This concern is highly important to address, because non-state actors today are capable of achieving damage on a severe and grave level, which was previously reserved to states only.[184] Non-state actors are not parties to the UN Charter and Article 2(4) does not apply to them.[185] However, after the events of 9/11, the UN Security Council adopted two resolutions that arguably recognize the right to self-defense against non-state actors in the context of international terrorism.[186] The role of non-state actors in cyberspace is part of a bigger phenomenon, often referred to as the "diffusion of powers."[187] According to Joseph Nye, a professor at the School of Government at Harvard University, there is a shift of powers from states that had monopoly over power to non-state actors that have recently found power more and more accessible. Nye comments on the role of non-state actors and explains, "the barriers to entry in the cyber domain, however, are so low, that non-state actors and small states can play significant roles at low levels of cost."[188] With regard to the power itself, Nye mentions: "[W]hat is distinctive about power in the cyber domain is not that governments are out of the picture, as the early cyber libertarians predicted, but that different actors possess different power resources and that the gap between state and non-state actors is narrowing in many instances."[189]

One way to overcome the difficulty of attribution when the state did not have effective control over the perpetrators' actions is to employ a flexible understanding of the attribution requirement in cyberspace. The law of attribution developed in a time where state involvement was obvious and easy to prove. The rise of powerful non-state actors who possess destructive cyber powers calls for an adjustment of the law of attribution. In the *Corfu Channel* case, the International Court of Justice affirmed "[E]very State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[190] Therefore, a state that knows of an individual or a group plans to launch a cyber attack, and is not acting under the governmental control, must take all necessary and reasonable measures to prevent such cyber attacks from being carried out. However, not all states that know of a non-state actor—within their territories—that launches a cyber attack or is expected to launch one are willing to take action. Sometimes, such states are unable to take action, not because they refuse to do so, but because they are incapable of doing so, militarily, financially or logistically. In such circumstances, victim states can be given the right to exercise what is known as the "extraterritorial law enforcement."[191] Dinstein mentions that in those circumstances, victim states "must [not] patiently endure painful blows, only because no sovereign State is to blame for the

184 *Information Warfare and International Law on the Use of Force*, *supra* note 13, at 108.
185 *Id.* at 72.
186 S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sep. 12, 2001); S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sep. 28, 2011).
187 JOSEPH NYE, THE FUTURE OF POWER 113 (2011).
188 *Id.* at 124.
189 *Id.* at 132.
190 *Corfu Channel Case (UK v. Albania)*, Judgment, 1949 I.C.J. 4, 22.
191 DINSTEIN, *supra* note 35, at 268.

turn of events."[192] In the ICJ Armed Activities case, Judge Kooijmans and Judge Simma emphasized the importance of not leaving a victim state helpless, saying "[I]t would be unreasonable to deny the attacked State the right to self-defence merely because there is no attacker state, and the Charter does not so require."[193]

However, the option of the extraterritorial law enforcement is not a *carte blanche* to self-defense against non-state actors, but it is a rather narrowly-structured exception to overcome very concrete situations. Extraterritorial law enforcement should be limited to responses to armed attacks carried out by non-state actors and only when such an armed attack is expected to recur; the victim state has to re-affirm the harboring state's unwillingness or incapability of taking action against the non-state actor.[194] The victim state should also first seek the harboring state's consent to the law enforcement action, and such an action should be proportionate, limited to the threat and necessary, which means that alternative *effective* measures should be weighed first.[195]

The drafters of the *Tallinn Manual* were aware of the attribution problem. However, it seems that little was done in regard to the adjustment of the law of attribution to cyber attacks. It appears that more restrictions were put upon victim states in their process of identifying the perpetrators of a cyber attack. We proceed to examine *Tallinn Manual*'s interpretation and addition to the law of attribution.

4.3.2. The Tallinn Manual on State Responsibility

Chapter one, section two of the *Tallinn Manual* deals with state responsibility. This section contains four rules. The first one (Rule 6) deals with the legal responsibility of states; the second and third rules (Rules 7 and 8) analyze the cyber operations launched from the governmental cyber infrastructure and cyber operations routed through a state, respectively, and the fourth rule (Rule 9) discusses countermeasures.

Rule 6 of the *Tallinn Manual* states, "[A] State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[196] Therefore, it is clear that cyber operations that reach the level of the use of force would be a breach of Article 2(4) of the UN Charter. This conclusion is based on the customary international law understanding of State responsibility. As stipulated in Article 2 of the Draft Articles on the *Responsibility of States for Internationally Wrongful Acts*, a state is responsible when the act or omission is attributable to the state under international law, and when it constitutes a breach of an international obligation of the state.[197] However, not all cyber operations originating in a state will hold it responsible under international law. As stated above, the use of force refers to the use of armed force, and therefore, unless otherwise prohibited in international law, a state would not be held responsible for the use of economic or political force through cyber operations, or for the use of

192 *Id.* at 269.
193 *Congo*, 2005 I.C.J. at 358, 370.
194 *See* Dinstein, *supra* note 35, at 275.
195 *Id.* at 275.
196 *Tallinn Manual*, *supra* note 10, at §6.
197 ILC Draft Articles, *supra* note 99, at §2.

cyber operations in espionage.

Rule 7 reads, "[T]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with the operation." Rule 8 reads, "[T]he fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State." Those rules do not seem to have a well-established international law source, but rather express an understanding as to the difference between the traditional usage of governmental infrastructure, i.e. the use of specific state-owned weapons on one hand, and the use of governmental cyber infrastructure on the other, which does not necessarily indicate state involvement. The commentary to Rule 7 explains:

> Prior to the advent of cyber operations, the use of governmental assets, in particular military equipment, would typically have been attributed to the State without question because of the unlikelihood of their use by persons other than State organs or individuals or groups authorized to exercise governmental functions. This traditional approach cannot be followed in the cyber context. It may well be that government cyber infrastructure has come under the control of non-State actors who then use that infrastructure to conduct cyber operations.[198]

Unlike Rule 7, which behaves toward the usage of governmental cyber infrastructure in an impermissible manner to assume State responsibility, Rule 8 deals with cyber operations, which are merely *routed* through a state cyber infrastructure. Such cyber operations do not use governmental cyber infrastructure in a direct fashion, but rather the data is passed through a state cyber infrastructure, whether governmental or non-governmental. The *Tallinn Manual* adds that the Group of Experts were unable to reach a consensus as to whether a state will still be held responsible for not preventing a cyber operation that is routed through its cyber infrastructure.

The Group of Experts is concerned that states might be hasty in wrongfully attributing a cyber operation to a state, which is understandable especially because cyber operations can be routed through the infrastructure of third states. However, Rules 7 and 8 do not reflect any customary international law norms or treaty law. The *Tallinn Manual* was intended to reflect existing international law norms that apply to cyber warfare. The inclusion of Rules 7 and 8 has greatly complicated the attribution task of the victim state, rather than simplify it. As mentioned above, the attribution requirement is tricky in the cyberspace context, and burdening it even more would leave victim states helpless should a cyber attack occur. Moreover, attacking states will refer to Rules 7 and 8 to deny their involvement in the cyber attack.

4.4. ANTICIPATORY SELF-DEFENSE AGAINST IMMINENT CYBER ATTACKS

Unlike traditional warfare, in the cyber context it could be tricky to act in anticipatory self-

198 *Tallinn Manual*, *supra* note 10, at §7, commentary 3.

defense, since the lapse of time between the decisions involving the engagement in a cyber-armed attack, the execution and the consequences of the attack is all a matter of milliseconds.[199] As such, the instances in which a state will successfully defend itself against an imminent cyber attack are uncommon.

However, a broader theory of anticipatory self-defense, also known as the "Bush Doctrine" allows engaging in self-defense against the threats that are not necessarily imminent. In 2002, the National Security Strategy stated: Security Strategy stated:

> We must be prepared to stop rogue states . . . before they are able to threaten or use weapons… Legal scholars and international jurists often conditioned the legitimacy of pre-emption on the existence of an imminent threat . . . We must adapt the concept of imminent threat to the capabilities and objectives of today's adversaries . . . The greater the threat, the greater is the risk of inaction - and more compelling the case for taking anticipatory action. [200]

Although the Bush doctrine has many opponents, it represents a viable concern with regard to cyber warfare. Cyber warfare poses a threat not only when imminent, but also when non-state actors and hostile states acquire the knowledge and technology to carry out such attacks. However, the Bush Doctrine represents one response of a state to threats, but as *Greenwood* posits, "[I]n so far as talk of a doctrine of "pre-emption" is intended to refer to a broader right of self-defence to respond to threats that might materialize at some time in the future, such a doctrine has no basis in law."[201]

The lack of imminence in cyberspace calls for a change of the understanding of anticipatory self-defense, as to make it more flexible and adapted to the new reality. However, on the other hand, providing states with the right to defend themselves against ambiguous and not yet materialized threats runs the risk of unnecessary uses of force, as well as escalations in hostilities. It remains to be seen how the international community will respond to the threat of cyber warfare. The response can be either restrictive to avoid the risk of more uses of unnecessary force, or it can be broad and flexible, in order to address the fear that many states have against the cyber warfare that will be targeted at them.

5. Conclusion

This thesis demonstrates that while the applicability of the *jus ad bellum* is important, the consequences and challenges of the application of the *jus ad bellum* on cyber warfare are uneasy, and as Hollis puts it, "even if it applies to [information operations], the existing system suffers from

199 *See Quo Vadis*, *supra* note 39, at 14.

200 White House, *The National Security of the United States of America*, 15 (White House, 2002) www.au.af.mil/au/awc/awcgate/nss/nss_sep2002.pdf (last accessed April 19, 2014).

201 Christopher Greenwood, *International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida, and Iraq*, 4 San Diego Int'l L. J. 7, 15 (2003).

several, near-fatal conditions: uncertainty… complexity… and insufficiency."[202]

It is clear that the *jus ad bellum* applies to cyber warfare. While the instrument-based approach is outdated and under-inclusive, the target-based approach is over-inclusive encompasses a wider array of cyber attacks that will be considered use of force. This will negatively broaden the scope of applicability of the use of force paradigm. The effects-based approach seems the most feasible approach to deal with cyber warfare; however, it remains to be developed further and reach wider consensus on the concretization of the use of force assessment.

From the institutional international law making perspective, the *Tallinn Manual* lacks the wide representation of nations. This NATO-sponsored effort to clarify international law applicable to cyber warfare is not always successful. As discussed in this thesis, while it makes sense to evaluate a situation involving the use of force by its scale and effects (i.e. the effects-based approach), the international law origin of the specific criteria developed in the *Manual* is unclear. Moreover, the criteria cause ambiguity and do not necessarily contribute to the understanding of the law. The *Tallinn Manual* is not the first instance in which international law is developed by experts. Such efforts were also carried out in the ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities, as well as the International Law Commission and many more. However, those represented a wide array of experts and perspectives, resulting in a relatively balanced and unbiased interpretation of the law. In order to overcome the challenges that the *Tallinn Manual* poses as an instrument, the international community needs to cooperate and engage in a treaty-making process. Such a process will most likely reach different understanding on what the international law applicable to cyber warfare is, and it will also represent the view of the international community as a whole. Moreover, even if the treaty will not be signed and ratified by every single state there is, it will still have legitimacy and a soft-law weight for the states that are not parties to the treaty.

As far as the substance is concerned, some recommendations are necessary to overcome the challenges discussed in this thesis. First, with regard to attribution, the *Tallinn Manual* could have established permissible and impermissible methods of attribution. Some methods of tracing back a cyber attack might constitute an act of an impermissible intervention. There must be a clear framework the methods that are permissible when a victim state traces back the attack, in order to identify the perpetrator. Moreover, the attribution in cyberspace should be read in the light of the first chapter of the *Tallinn Manual*, which emphasizes the state's duty to exercise sovereignty and prevent cyber attacks from being conducted or routed through its infrastructure. If states are cautious and do all they can to prevent cyber attacks that are routed or carried out from their territories, then it will minimize potential cyber attacks carried out by non-state actors who are not under the control of that state. The *Tallinn Manual* prevents attribution on the grounds of mere routing or the origin of a cyber attack (Rules 7 and 8), but it seems that attribution should be

202 Duncan Hollis, *New Tools, New Rules: International Law and Information Operations*, G.J. David and T.R. McKeldin (eds.), IDEAS AS WEAPONS: INFLUENCE AND PERCEPTION IN MODERN WARFARE 60 (2004).

performed on a case-by-case basis and of the available evidence and circumstances.

Second, if the *jus ad bellum* is focused today on the effects, rather than the instrument employed, there is no escape from including political and economic coercions in the scope of the use of force. Cyber attacks allow rather easy and accessible political and economic coercions, and as demonstrated in the Syrian Electronic Army case example, economic coercion may have similar effects to a physical armed coercion. The severity of a cyber attack targeting major financial institutions or governmental infrastructure could be devastating, and excluding those from the scope of the use of force (and leaving it in a legal vacuum) is not in conformity with the goals and spirit of the UN Charter and the international community values. The criteria set forth in the *Tallinn Manual* require more refinement. The weight of each criterion is vague and the origin of most of them is ambiguous. There are many other criteria that could be considered in the effects-based approach, such as the expected damage from the attack, how easily the damage can be averted, the collateral damage and several others. However, it is clear that the severity of the cyber attack is the most significant factor in the process of evaluation.