Name:	Tshepo Tlhacoane
Student Number:	TLHTSH006
Degree:	Master of Laws, Specialising in International Law
Title:	Cyberattacks: The latest threat to international peace and security, and how international law can respond
Supervisor:	Dr. Cathleen Powell
Word count:	22018/25000

Research dissertation/research paper presented for the approval of Senate in fulfilment of part of the requirements for the in approved courses and a minor dissertation/research paper. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of dissertations/research papers, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation/research paper conforms to those regulations.

Date: Signature: Signed by candidate

‘I believe the target of anything in life should be to do it so well that it becomes an art.’ - Arsène Wenger

ABSTRACT

Today it is accepted that states may not unilaterally attack each other using rifles, missiles, nuclear, or chemical weapons. But what about computer software such as worms and trojans which are capable of causing similar or greater damage? Are states permitted to attack each other using these so-called cyberweapons? Are they even considered weapons due to their differing form? This is the crux of what this dissertation is about. It aims to show that if states are prohibited from attacking each other with certain categories of weapons, they should not be permitted to attack each other with a different weapon which causes similar damage. I make three overarching arguments in this dissertation. The first is that cyberweapons should be considered ‘weapons’ even though they differ in form and sophistication. Secondly, that the use of cyberattacks is a use of force and contravenes article 2(4) of the UN Charter. Finally, I will argue that extant international law is not able to maintain international peace and security and that a multilateral treaty is required.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

In February 2019, reports emerged in various media outlets that Russia was planning on shutting down the internet within the country temporarily in order to simulate an all-out cyberwar.[1] These reports suggest that the shutdown appears to be a test by the Kremlin in preparation to wean Russia off foreign internet service providers and make Russia digitally independent in a bid to protect the country against cyberattacks.[2] These developments appear to be in line with the cyber defence policy which the Russian government has been working on for numerous years,[3] with some Russian officials saying that Russia aims to have 95% of all internet traffic routed locally by 2020.[4]

To the layperson, Russia's decision to remove and insulate itself from the internet may be seen as drastic, but upon closer inspection, Russia's actions may be viewed as pre-empting the latest threat to international peace and security: cyberattacks.

The advancement of technology has impacted all aspects of life. Conflict and weaponry are no different. Cyberspace is increasingly becoming the battleground where states and non-state actors look to engage in conflict, and this is supported by William Boothby who said:

> The rifle, the bayonet, mortars, bombs, missiles, and mines will remain critically important tools in the conduct of hostilities in many future, conventional armed conflicts… But cyberspace will… become the environment in which adversaries employ some degree of operational sophistication and will seek to gain and maintain military advantage by leveraging their own hostile activities while impeding the enemy's capability to organize and operate.[5]

---

[1] Alex Kimani 'Why is Russia turning off its internet?' *Safehaven Preservation of Capital* 16 February 2019 available at *https://safehaven.com/news/Breaking-News/Why-Is-Russia-Turning-Off-Its-Internet.html* accessed 16 May 2019.
[2] Ibid.
[3] Harry Pettit 'Cyberwars Russia to test to test turning the entire internet OFF to defend against US cyberattack' *The Sun* 11 February 2019 available at *https://www.thesun.co.uk/tech/8401797/russia-vs-us-cyber-war-games/ accessed* 16 May 2019.
[4] Ibid.
[5] Claire Oakes Finkelstein and Kevin H. Govern 'Introduction: Cyber and the Changing Face of War' (2015) *Penn Law Faculty Scholarship Paper* at xx.

Cyberattacks are no longer a hypothetical possibility. Cyberattacks are a reality. Furthermore, cyberattacks are no longer limited to gathering sensitive information from one's adversaries but are now used to cause physical damage to one's enemies. There are plenty of examples of states and non-state actors who have conducted cyberattacks which caused physical damage, the most prominent being 'Operation Olympic Games' which was orchestrated by the United States and Israel against Iran.[6]

This attack involved releasing a virus into the computer systems of the nuclear reactor at Natanz which was considered to be the central facility for uranium enrichment for Iran's nuclear weapons.[7] The virus wreaked havoc and caused damage to critical infrastructure, and other damage which was comparable to an attack using traditional weapons. Former CIA Director Michael Hayden summed up the importance of this attack when he said, 'this is the first attack of a major nature in which a cyberattack was used to effect physical destruction.'[8] He would later compare this transformation in warfare to that which occurred in 1945 after the development and use of the atomic bomb.[9] This sentiment was echoed by former FBI Director Robert Muller who said that a cyberattack could have the 'same impact as a well placed bomb.'[10]

Unlike nuclear and other weapons of mass destruction which were only available to a relatively small number of states, cyberattacks can be employed by most states. In 2007, security firm McAfee estimated that 120 states had developed ways to use the internet to target financial markets, government computer systems and utilities.[11] Iran has previously boasted about having the world's second largest cyber army.[12] The

[6] Jens David Ohlin, Kevin Govern, and Claire Finkelstein *Cyberwar: Law and Ethics for Virtual Conflicts* (2015) at ix.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Reuters 'FBI Director Robert Mueller warns of growing cyber threat, could affect gov't, business, individuals' 5 March 2010 *NY Daily news* available at *https://www.nydailynews.com/news/money/fbi-director-robert-mueller-warns-growing-cyber-threat-affect-gov-business-individuals-article-1.174257* accessed on 16 May 2019.
[11] Ohlin, Govern and Finkelstein op cit note 6 at ix.
[12] Ibid.

threat of cyberattacks and cyberwar is so great to the United States that the FBI considered them the number one threat to US national security.[13]

The preceding paragraphs raise numerous questions. First, are the tools used to carry out cyberattacks (cyberweapons) considered weapons in the same way as traditional weaponry? Second, are the use of cyberattacks a use of force, and therefore a contravention of article 2(4) of the UN Charter? Finally, if cyberattacks are a use of force, is existing international law capable of adequately regulating interstate conflict in the new battleground of cyberspace?

This dissertation will make three overarching arguments: the first is that cyberweapons are weaponry and should be regarded as weapons in the same way as traditional weapons. Second, that cyberattacks are a use of force. Finally, I will argue that existing international law is not able to adequately regulate the use of cyberattacks and that a multilateral treaty is required to maintain international peace and security.

This dissertation will therefore be divided as follows: chapter two will argue that cyberweapons are weapons, and it will provide examples of states using them as such. The purpose of this chapter is two fold: first, it is to establish what a cyberweapon is as there is no international consensus on the meaning of both 'weapon' and 'cyberweapon'. Second, this chapter aims to show that states are using cyberweapons alongside, or as an alternative to traditional weapons. This Chapter will also provide the reader with examples of the different types of cyberweapons. Finally, this chapter will provide numerous examples of states employing cyberattacks.

Chapter three will argue that cyberattacks can constitute an armed attack, or what the ICJ in the *Nicaragua* case[14] termed the 'most grave' use of force.[15] This will build on chapter two, which discusses the physical damage that can be caused by cyberattacks, and that such cyberattacks can cause damage of the *scale and effects* required to constitute an armed attack.

---

[13] RT 'FBI: Cyber Attacks – America's Top Terror Threat' 2 March 2012 available at *https://www.rt.com/news/cyber-fbi-security-mueller-691/* accessed on 31 March 2019.
[14] *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States) (1986) ICJ.
[15] Ibid para 191.

Chapter four will argue that cyberattacks can also constitute a ‘less grave’ use of force. This chapter may initially seem redundant because a cyberattack which is an armed attack by extension satisfies the requirements to be a ‘less grave’ use of force. However, it is still worth investigating the status of cyberattacks which do not rise to the *scale and effects* to constitute an armed attack, and to investigate the non-violent cyberattacks and whether they too can constitute a use of force.

Chapter five will argue that existing international law is not able adequately to deal with the unique nature of cyberattacks, and that a multilateral treaty is the best option to maintain international peace and security. In making this argument, this section will discuss the judicial and non-judicial responses currently available to the victim state of a cyberattack. This chapter will then discuss numerous ways in which a multilateral treaty would better address state conduct in cyberspace, thereby ensuring the maintenance of international peace and security.

Chapter six will be the final chapter of this dissertation and will discuss the conclusions reached throughout the course of this dissertation.

CHAPTER TWO: CYBERWEAPONS AND CYBERATTACKS

In this chapter, I plan to make the first of my three overarching arguments, which is to argue that cyberweapons are weapons. The aim of this chapter is to argue that the concept of a 'weapon' is not static, but is ever evolving and includes cyberweaponry. This chapter's aim is to argue that despite differing in form and sophistication, cyberweapons form the latest development of the evolution of weaponry. This is supported by the fact that states have added cyberweaponry to their arsenals and are using cyberweapons alongside, or in place of traditional weapons. This sentiment is echoed by international law expert, Professor Yoram Dinstein who said:

> Weapons (including munitions) are the means of warfare, and without weapons there can be no war. Weapons determine the way war is fought – on land, at (or under) the sea, and in the air – and frequently their outcome. History is replete with illustrations of weapons affecting civil life (for instance, the appearance and disappearance of walled cities) and the formation of empires (for example, the need of navies for coaling stations). Military history is a history of changing weapons. Mankind has come a long way from sling stones or bows and arrows to nuclear weapons, and the rapid pace at which novel weapon systems emerge in the modern era of computers and electronics is unprecedented.[16]

Arguing that cyberweapons are weapons is complicated by the fact that there is no internationally accepted definition for both 'weapon' and 'cyberweapon'.[17] Surprisingly, these terms are also not present in the latest version of the US Department of Defence's Dictionary of Military Terms.[18]

In arguing that cyberweapons are weapons, this chapter will be divided as follows: Section A will define and discuss cyberweapons. Section B will proceed to set out some of the types of cyberweapons which have been identified. Finally, Section C will provide examples of states using cyberweapons either alongside, or in place of traditional weaponry.

---

[16] William H. Boothby *Weapons and the law of armed conflict* 2 ed (2016) at vii.
[17] Thomas Rid & Peter McBurney 'Cyber-weapons' (2012) *The Rusi Journal* at 6.
[18] United States Department of Defence 'DOD Dictionary of Military Terms' (2018) available at *https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf* accessed 12 August 2019.

SECTION A: CYBERWEAPONS

One of the most surprising discoveries of this investigation has been the lack of an internationally accepted definition of what a weapon is. This is because of mankind's prolonged use of weaponry and because so many international conventions ban or regulate the use of certain weapons.

Moving forward, this dissertation will rely on the following definition when discussing traditional weapons: a weapon is a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems, or living things.[19] This definition is deemed satisfactory because it covers tools that are intuitively understood to be weapons such as rifles and other firearms, but it is also able to cover tools which were not created to be weapons but which have been repurposed with the intention of being used as weapons, such as a knife or a hammer.

Cyberweapons differ too much in form and sophistication from traditional weapons to completely fall under the above definition. Instead, Rid and McBurney provide the following definition of a cyberweapon: 'a cyberweapon is seen as a subset of weapons more generally: as a computer code that is used, or designed to be used, with the aim of causing physical, functional or mental harm to structures, systems or living beings.'[20]

This definition (malicious software + intention) is supported by other authors such as Louise Arimatsu who defines a cyberweapon as 'malicious code with offensive capabilities.'[21] She continues to say that it is 'both the intended outcome or effects produced by that code that transforms it into a weapon that should be governed, as with conventional weapons, by the law of armed conflict.'[22]

Cyberweapons differ from traditional weapons in that traditional weapons are intended to cause *direct* physical damage which would lead to the death or injury of persons and the destruction of property. Cyberweapons on the other hand are intended to have an *indirect* outcome which may then result in death, injury or

---

[19] Thomas Rid & Peter McBurney Op Cit note 17 at 7.
[20] Ibid.
[21] Louise Arimatsu 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' (2012) *NATO CCD COE Publications* at 98.
[22] Ibid.

destruction of property. Although cyberweapons are intended to cause an indirect outcome, the devastation can be similar or greater than that which traditional weapons could cause. The worst case scenarios that have been envisaged would be overriding the controls at a nuclear or chemical powerplant which would cause a chemical release or nuclear meltdown killing thousands, if not millions of people.[23] The next section will discuss some identified cyberweapons.

SECTION B: TYPES OF CYBERWEAPONS

This section aims to discuss three types of cyberweapons: viruses and worms; trojans and rootkits; and botnets. This list does not represent all cyberweapons, but merely the most widely known and utilized.

(a) Viruses and Worms

In the same way that biological viruses attach themselves to larger organisms and feed off them, a computer virus infects a program or file, abuses it to spread itself, and inflicts damage ranging from system malfunction, system shutdowns, data corruption and erasing.[24]

Worms are stand-alone viruses that are not attached to any files.[25] They are small hidden programmes that remain inactive until certain conditions are met, or when they have been remotely activated.[26] They self-replicate and exploit software flaws and other weaknesses in emails, unattended ports or buffer overflows.[27]

(b) Backdoors: Trojans and Rootkits

This software, which was named after the infamous Trojan horse, is a program that either poses as a legitimate free software, or hides in a legitimate looking file.[28] The user is then enticed into installing the programme and is lured into opening a file containing a Trojan. Once installed, the Trojan secretly performs its tasks, which include but are not limited to, capturing data such as login credentials, credit card

---

[23] Council on Foreign Relations 'Cyberterrorism Hype v. Fact' available at *https://www.cfr.org/expert-brief/cyberterrorism-hype-v-fact* accessed on 12 August 2019.
[24] Georg Kerschischnig *Cyberthreats and international law* (2012) at 31.
[25] Ibid.
[26] Ibid at 32.
[27] Ibid.
[28] Ibid.

information, and trade, military and state secrets.[29] Trojans usually open a 'backdoor' to the infected system so that the perpetrator can update and revise it to avoid security programmes designed to detect and remove them.[30]

A 'rootkit' refers to a special kind of Trojan that may be installed by a hacker who has gained access to a computer system.[31] Like a Trojan mentioned above, it creates a backdoor and remains hidden to the user by staying invisible in the list of processes and services.[32] It gives the hacker access to the compromised system and then awaits further instructions from the hacker, such as downloading additional malware.[33]

(c) Botnets

Bots, which derive from 'robots', are a special kind of Trojan which take control of a small number of the infected system's resources and allocate them to their 'master' who controls a network of infected systems.[34] The affected computers become so-called 'zombies' and the abovementioned master controls all of his zombies in a botnet.[35] A botnet therefore can be understood as a network of bots.

Botnets are able to take instructions from any infected computer and can infect computers in a number of ways, but mainly through always-on broadband connections.[36] A newer trend does not even require that the computers be switched on in order to be infected and for the perpetrator to assume control. Here, the perpetrator assumes control over modems, routers, and satellite TV receivers.[37] What makes this an attractive method is that in private homes, these devices are more likely to be switched on all the time and remain connected to the internet for much longer periods.[38]

Botnets have a variety of capabilities. They can be used to spy on infected machines and collect personal information, to create backdoors to gain further access to a compromised system, to use an infected system as an intermediary when breaking

[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Ibid at 33.
[34] Ibid.
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.

into other systems (thus covering their tracks), or to launch Distributed Denial of Service (DDoS) attacks.[39] DDoS attacks are generally launched against servers, and not a single computer. When an attack hits a server, it receives more requests than it can handle, leading to delays or to the server's complete incapacity until the requests start to decrease. Their aim is to temporarily affect the availability of a system or network and they can be used to stall or take down the targeted system, prevent communication and cause a network and even parts of the internet to slow down.[40] A practical example of this was during the cyberattacks on Estonia, which will be discussed in greater detail below.

Botnets entangle thousands of computers and have gained popularity recently, and their popularity is a cause for concern as they can easily infect a system while browsing legitimate but infected sites.[41] In 2009, the Georgia Tech Information Security Centre estimated that these bots affected 15% of all computers online. This means that hypothetically speaking, there existed a bot army that could have been used in a cyberwar.[42]

Their efficiency is also a cause for concern for security experts. A research group managed to get temporary access to a botnet, and in 10 days they were able to collect 70GB off data which, when extracted, gave them access to the credentials of 8310 financial accounts, 1660 credit and debit card numbers, and 297,962 user credentials.[43] This concern is further exacerbated by the recent trend of renting out botnets and associated services, and it appears that botnets seem to be becoming more resilient against efforts to take them down.[44]

SECTION C: EXAMPLES OF CYBERATTACKS

The main reason that I argue that cyberweapons are to be considered weapons like traditional weapons is because they are considered so and are used as such. Evidence of the militarization of cyberspace is best articulated by retired US Air Force General and the Former Director of the National Security Agency, Michael Hayden who said:

---

[39] Ibid.
[40] Ibid at 35.
[41] Ibid at 34.
[42] Ibid.
[43] Ibid.
[44] Ibid.

> Like everyone else who is or has been in a US Military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air space, cyber. It trips off the tongue, and frankly, I have found the concept liberating when I think about operationalizing this domain.[45]

Former US President Barack Obama also famously referred to cyberweapons as "weapons of mass disruption" in a speech in 2009.[46] The rest of this section will discuss various examples where states used cyberweapons either alongside, or as an alternative to traditional weapons.

(a) Siberia, 1982

On 21 September 1982, a three kiloton explosion tore apart a natural gas pipeline in Siberia. The explosion was so large that it was visible from outer space and is considered the most monumental non-nuclear explosion and fire ever seen from space.[47] Despite suspicions that the perpetrator was the US, the lack of proof linking them to the act meant that it could only remain speculation.

In 2004, it was revealed that the attack was instigated by the CIA,[48] when former Senior NSA official Thomas Reed revealed in his book that the US allowed the USSR to steal pipeline control software which contained a Trojan that caused an explosion in the Trans-Siberian pipeline.[49] The Trojan did so by making the valves, pumps and turbines act erratically and produce pressures far beyond those acceptable to pipeline joints and welds.[50]

---

[45] Martin C. Libicki 'Cyberspace Is Not a Warfighting Domain' (2012) I/S: *A Journal of law and Policy for the Information Society* available at *https://pdfs.semanticscholar.org/8efa/452e76f1666ab4efd2f10276078a430486f1.pdf* at 321.
[46] Politico 'Weapons of Mass Disruption' (2009) available at *https://www.politico.com/story/2009/05/weapons-of-mass-disruption-023099* accessed 12 August 2019.
[47] David E. Hoffman 'Reagan Approved Plan to Sabotage Soviets' *The Washington Post* 27 February 2004, available at *https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/?noredirect=on* accessed on 12 August 2019.
[48] Ibid.
[49] Risi 'CIA Trojan Causes Siberian Gas Pipeline Explosion' available at *https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion* accessed 2 august 2019.
[50] Ibid.

(b) Estonia, 2007

In 2007, Estonia was a victim of a cyberattack the likes of which had never been seen before. Its effects were compounded by the fact that Estonia at that time, had the reputation of being the most connected country in Europe.[51] The importance of this attack was described by Wired magazine as follows:

> This was not the first botnet strike ever, nor was it the largest. But never before had an entire country been targeted on almost every digital front all at once, and never before had a government itself fought back. The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia […]. All major commercial bank, telecos [telecommunication providers], media outlets and name servers – the phone book of the internet – felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.[52]

In this attack, which occurred after the relocation of a Soviet war memorial, botnets commanded computers all over the world to attack Estonian websites with bogus traffic,[53] while hackers targeted banks, governmental services, media providers, and even the national emergency call numbers.[54] The Defence Minister even said 'people felt that there was a real threat to national security.'[55]

Estonian officials openly accused the Russian government from the outset of the attacks. However, no direct involvement of the Russian government was ever established.[56] Only one person, an Estonian student of Russian heritage was convicted for participating in the attacks[57]

(c) South Ossetia War, 2008

The summer of 2008 was characterized by tensions between Georgia and Russia concerning South Ossetia and Abkhazia. This conflict is significant because it is the

[51] Georg Kerschischnig Op Cit note 24 at 61.
[52] Ibid.
[53] Ibid at 62.
[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Ibid.

first time that cyberattacks had not only preceded a conventional war for approximately two months, but intensified and ran parallel with it and even continued after the war was over.[58] It was also the first time in which a ground attack coincided with a cyberattack.[59]

The damages to Georgia were not as severe as Estonia because it was not as developed in terms of the internet. Therefore, the damage Georgia suffered was mainly to the disruption of governmental communication channels, media outlets, banks and transportation providers.[60] Georgian hackers retaliated by attacking Russian news outlets and the South Ossertian government, however, they were 'outgunned' by their opponents.[61]

(d) Iran, 2010

The cyberattack on Iran in 2010 was briefly discussed in the first chapter. However, the first chapter discussed the effects of the cyberattacks, while this section aims to discuss the technological aspects of the cyberweapon which were omitted in the first chapter.

This attack gained infamy for the use of the 'Stuxnet' worm, which specifically targeted critical infrastructure.[62] Stuxnet is a highly infectious self-replicating computer worm that disrupted the Iranian nuclear plant.[63] It took control of the computers, altered the speed of the centrifuges in the plant and shut them down.[64]

Stuxnet hid on USB flash drives and installed upon attachment to the computer where it was able to exploit four zero-day vulnerabilities (a software security flaw known to the vendor, but the software vendor doesn't have a patch to fix the flaw)[65] which was highly unusual.[66] It continued to surprise cybersecurity specialists as it was discovered that this worm had the ability to make modifications in systems and

---

[58] Ibid at 63.
[59] Jonathan A. Ophardt 'Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield' (2010) *Duke Law & Technological review no 3* at 2.
[60] Georg Kerschischnig Op Cit note 24 at 63.
[61] Ibid.
[62] Ibid at 69.
[63] Norton 'Zero-day Vulnerability: What is it, and How it Works' available at *https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html* accessed 3 August 2019.
[64] Ibid.
[65] Ibid.
[66] Georg Kerschischnig Op Cit note 24 at 69.

that its exact capabilities remained unknown, although experts speculate that it could have led to serious physical effects.[67]

Stuxnet was also designed to target only industrial systems provided by Siemens, and only if certain conditions were met such as geographic location.[68] This meant that it was designed to target systems which specifically controlled oil pipelines, electric plants, nuclear facilities and other large industrial installations.[69] Investigations revealed that Stuxnet neutralized with the frequencies of enrichment centrifuges which could cause them to malfunction, or even destroy them.[70]

CONCLUSION

This chapter sought to argue that cyberweapons are weapons. Despite being different in form and sophistication from traditional weapons, I submit that they are to be viewed as the latest development on the weapons spectrum as opposed to being a different entity.

This argument is supported by other authors who have written on the matter who submit that a cyberweapon is malicious software which is intended to cause harm. It is also supported by state practice. This chapter has provided several examples of states utilizing cyberweaponry either alongside traditional weapons, or as alternatives to traditional weapons. Although they differed in form, cyberweapons were able to cause damage comparable to traditional weapons with the benefit of the perpetrator not needing to be in (relatively) close proximity to launch the attack.

I submit that this chapter achieved its primary purpose which was to support the first of my overarching arguments that cyberweapons are weapons. By achieving its primary objective, this chapter has also created the perfect segue for the second of my arguments: that cyberattacks are a use of force.

---

[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Ibid.

CHAPTER THREE: ARE CYBERATTACKS AN ARMED ATTACK?

As a result of the Second World War and numerous attempts before that to limit war between states, Allied Powers drafted and adopted the UN Charter, containing an all-encompassing prohibition of the use of force in article 2(4). Although it has been over 70 years since the Charter was adopted, the term 'force' is still surrounded by ambiguity. However, the majority of commentators consider the term 'force' in article 2(4) of the Charter as being synonymous with 'armed' or 'military' force.[71]

This interpretation of force might have been sufficient in the aftermath of the Second World War as armed or military force was the only way in which states engaged in conflict. But technological advancements since the end of the Second World War have led to the emergence of a new domain where states can engage in conflict, cyberspace. The emergence of this new domain and its use by states to attack one another raises an important legal question: are cyberattacks a use of force according to article 2(4) of the UN Charter?

Intuitively, one would come to the conclusion that cyberattacks are a use of force for numerous reasons. First, article 2(4) is the primary norm entrusted to safeguard international peace and security,[72] and by becoming parties of the Charter, states accept a treaty law obligation to refrain from the threat or the use of force. Secondly, this provision – along with the overall aim of the Charter – aims to prevent interstate conflict and maintain international peace and security. Thirdly, as discussed in the previous chapter, cyberattacks are now no longer limited to hacking and other such intrusions, but are capable of causing physical damage similar to that caused by traditional weapons. Finally, I submit that the Charter would not be able to achieve its goal of maintaining international peace and security and 'saving succeeding generations from the scourge of war' if it allowed for the use of cyberattacks by states. I submit that this would eventually provoke military force and ultimately lead to the outbreak of an international armed conflict.

[71] Nils Melzer 'Cyberwarfare and International Law' *UNIDIR Resources* (2011) at 7.
[72] Ibid at 9.

Ascertaining whether cyberattacks are a use of force poses numerous challenges. The first is that there is no international consensus on a precise definition of a use of force both in and out of cyberspace.[73] Secondly, although an argument can be made that cyberattacks can be an armed attack based on its *scale and effects,* the real difficulty arises in classifying cyberattacks whose damage does not rise to the threshold of an armed attack, or cyberattacks which do not cause death, injury or destruction (non-violent cyberattacks).

Some legal experts have suggested that in order to qualify as a use of force, cyberattacks must have 'violent consequences.'[74] A significant problem with this view is that in a world of heavy economic, political, military and social reliance on the internet, the consequences of the non-violent cyberattacks could exceed the 'violent' ones.[75] humankind's ever-increasing reliance on the internet is exemplified by the fact that the 15 years between 1995 and 2010 saw the number of individuals who used the internet rise from 16 million to over 1.7 billion people.[76] Today, states, non-state communities, businesses, academia and individuals have become interconnected and interdependent in ways never imagined.[77] A consequence of this is that there are exponentially more potential 'targets' of a cyberattack, and the interconnectivity between people means that the collateral damage of a cyberattack could be catastrophic.

Based on the reasons listed above and those I will discuss below, the next two chapters will argue that cyberattacks are a use of force according to article 2(4) of the UN Charter. This chapter will focus on whether cyberattacks can amount to an armed attack or what the ICJ has termed the 'most grave' use of force. Chapter four will address whether cyberattacks are a 'less grave' use of force.

---

[73] Matthew C. Waxman 'Cyber-attacks and the use of force: Back to the Future of Article 2(4)' (2011) *Yale Journal of International Law* at 433.
[74] Ibid at 435.
[75] Ibid at 436.
[76] Nils Melzer Op Cit note 71 at 3.
[77] Ibid.

SECTION A: CAN CYBERATTACKS BE ARMED ATTACKS?

Having established in the previous chapter that attacks employed with cyberweapons (cyberattacks) can cause damage which is similar to, or in some cases greater than that caused by traditional weapons, the question which needs to be answered is what options are available to a state which is the victim of a cyberattack? Are victim states left with little option but to endure and tolerate cyberattacks against them, or can they use force in self defence?

In 2011, the US warned that it would retaliate with military force if it considered a cyberattack to be devastating enough.[78] In the UN Charter era, to legally adopt this position they would need to rely on article 51 of the UN Charter which recognises states' inherent right to individual and collective self defence. But this provision limits self defence to a state which has suffered an armed attack.

This section will argue that a cyberattack is capable of being an armed attack. Although cyberattacks are employed by both state and non-state actors, this chapter will only focus on cyberattacks between states, or those that can be attributed to a state. Cyberattacks by non-state actors such as terrorists, whose actions cannot be attributed to a state are beyond the scope of this chapter. Furthermore, this chapter will limit itself to whether a cyberattack can rise to an armed attack and will not discuss the considerations when acting in self defence, which are discussed in the *Caroline* case.[79]

The discussion below will be based on the *Tallinn Manual on the International Law Applicable to Cyber Warfare*[80] (Hereafter, the Tallinn Manual or the Manual) in order to argue that cyberattacks can be armed attacks triggering the right of self defence. The Tallinn Manual was written after the cyberattacks in Estonia at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. The Manual was written by 20 internationally renowned experts in order to ascertain how international law can apply to cyber operations and cyberwarfare. In addition to the experts, three organizations were represented by observers throughout

---

[78] Phil Stewart 'Analysis: Could a cyber war turn into a real one for the U.S.?' available at *https://www.reuters.com/article/us-usa-cyber-pentagon/analysis-could-a-cyber-war-turn-into-a-real-one-for-u-s-idUSTRE74U75420110531* accessed on 9 November 2019.
[79] *The Caroline v. The United States,* 11 U.S. (7 Cranch) (1813).
[80] Michael N. Schmidt *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013).

the drafting process. These organizations were NATO, which was represented by Ulf Häußler, the International Committee of the Red Cross which was represented by Dr. Cordula Droege and Dr. Jean-Francois Queguiner, and the United States Cyber Command which was represented by Colonel Gary D. Brown.[81] In an attempt to add academic credibility to the Manual, the Manual was peer reviewed by 13 international legal scholars prior to its publication.[82]

(a) Cyberattacks as armed attacks

Article 51 of the UN Charter allows for the unilateral use of force by states only when they have suffered an armed attack. This provision states that:

> Nothing in the present Charter shall impair the inherent right of individual or collective self defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace.

The experts confirmed that article 2(4) does not specify the type of weapon to be used in a use of force, and therefore an armed attack. This was confirmed by the *Legality of Nuclear Weapons*[83] case where the ICJ confirmed that the choice of weaponry was immaterial to whether an attack qualified as an armed attack.[84] This seems to be consistent with state practice where it is universally accepted that chemical, biological and radiological attacks of the *scale and effects* sufficient to constitute armed attacks trigger the right to self defence, despite their non-kinetic nature.[85] The experts submit that identical reasoning would apply to cyberattacks.[86]

In order for a state to rely on self defence, that state would need to be a victim of an armed attack which presupposes a use of force in the sense of article 2(4).[87] In the *Nicaragua* case, the ICJ noted that not every use of force amounted to an armed attack, and therefore a state was only entitled to invoke article 51 if it had suffered an armed attack.[88] Secondly, the Court found it necessary to distinguish the 'most

---

[81] Ibid at 7.
[82] Ibid at 7 and 8.
[83] *Legality of the Threat or Use of Nuclear Weapons* (1996) ICJ.
[84] Ibid Para 39.
[85] Michael N. Schmidt Op Cit note 80 at 54.
[86] Ibid.
[87] Ibid.
[88] Ibid.

grave' forms of the use of force (those constituting an armed attack) from 'less grave forms' such as a mere 'frontier incident' based on the '*scale and effects'* of the force involved, however the Court provided no further guidelines.[89]

It is unsettled as to how many deaths are required before a cyberattack can constitute an armed attack. However, Security Council Resolution 611 has shown that even the death of a single individual is sufficient to constitute an armed attack. This Resolution was adopted after Khalil al-Wazir, an affiliate of the Palestinian Liberation Organization was assassinated by Israeli forces and the Security Council declared this to be an act of aggression committed against the sovereignty and territorial integrity of Tunisia.[90] Additionally, the Security Council also referred to the attack as a 'flagrant violation of the Charter of the United Nations'.[91] That being said, the International group of experts agreed that some cases were clear and that a cyberattack that injures or kills people or damages property would satisfy the *scale and effects* doctrine as articulated in *Nicaragua*.[92]

According to the experts, an armed attack must have a trans-border element, and this element is always met when one state employs a cyberattack against another state which reaches the level of an armed attack.[93]

There was deliberation between the experts whether the notion of an armed attack, because of the word 'armed', necessarily required the use of a 'weapon'. The majority took the view that it did not, and that the critical factor was whether the effects of the cyberattack were comparable to those that would have arisen from an attack using traditional weapons.[94]

Another issue of importance is whether cumulative cyberattacks could rise to the threshold of an armed attack.[95] According to the experts, the determining factor is whether the same perpetrating state (whether directly or indirectly) has carried out smaller cyberattacks that are related, and that when taken together, meet the

---

[89] *Military and Paramilitary Activities in and Against Nicaragua* Op Cit note 14 Para 191.
[90] The next chapter will discuss how 'aggression' forms part of the article 2(4) prohibition.
[91] UNSCR 'Resolution 611' available at *http://unscr.com/en/resolutions/611* accessed 7 October 2019.
[92] Michael N. Schmidt Op Cit note 80 at 55.
[93] Ibid at 54.
[94] Ibid.
[95] Ibid at 55.

threshold.[96] If there is convincing evidence of this, then the experts agreed that there are grounds for treating the attacks as a composite armed attack.[97] This argument can find support in the *Oil Platforms*[98] case where the Court seemed to suggest that cumulative attacks can amount to an armed attack.[99]

A challenging issue regarding cyberattacks involves determining which adverse effects to consider when deciding whether a cyberattack qualifies as an armed attack. The group of experts agreed that all foreseeable consequences of the cyberattack qualify.[100] An example would be a cyberattack targeting a water purification plant. According to the experts, sickness and death caused by the contaminated water are foreseeable and should therefore be taken into consideration when deciding whether a cyberattack is an armed attack.[101] There was some division however, about whether the effects must have been intended. The majority of the experts took the view that intention was irrelevant and that only the *scale and effects* mattered.[102]

It is also necessary to consider the perpetrator when determining whether a cyberattack is an armed attack. In *Nicaragua*¸ the ICJ said that:

> An armed attack must be understood as including not merely action by regular forces across the international border, but also the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries which carry out acts of armed force against another state of such gravity as to amount to (*inter alia*) an actual armed attack conducted by regular forces, or its substantial involvement therein.[103]

Thus, if a group of private individuals under the direction of state A commit cyberattacks directed against state B, and the consequences of the attack reach the requisite *scale and effects*, state A will have committed an armed attack.[104] The same is true of a cyberattack conducted by an individual at the direction of a state.[105]

---

[96] Ibid.
[97] Ibid.
[98] *Oil Platforms* (Islamic Republic of Iran v. United States of America) (2003) ICJ.
[99] Ibid Para 64.
[100] Michael N. Schmidt Op Cit note 80 at 56.
[101] Ibid.
[102] Ibid.
[103] *Military and Paramilitary Activities in and Against Nicaragua* Op cit note 14 Para 195.
[104] Michael N. Schmidt Op Cit note 80 at 57.
[105] Ibid.

The exercise of self defence is subject to the existence of a reasonable determination that an armed attack has occurred as well as the identity of the attacker.[106] The issue regarding the inability to identify the perpetrator of a cyberattack is one that has plagued the debates surrounding cyberattacks. However, it seems as though advancements in technology have allowed states to be able to identify the perpetrators of cyberattacks. This was the case in October 2018 where the UK and its allies exposed a cyber campaign by the GRU - the Russian military intelligence service - which launched cyberattacks targeting political institutions, businesses, media and sports institutions.[107] These attacks attempted to undermine international sporting institution WADA, disrupt transport systems in Ukraine, destabilize democracies and target businesses. What was of importance here was the UK's ability to attribute numerous attacks to Russia with 'almost certainty',[108] meaning that perpetrators of cyberattacks may not be able to act with impunity in the future.

(b) Academic Response to the Tallinn Manual

The Tallinn Manual sought to show that existing international laws were applicable to cyberwarfare, and it has been met with both praise and critique. Those who praise it find it to be a 'useful compilation of rules with commentary reflecting the different views on some of the thorny issues raised by this new technology.'[109] Even critics of the Tallinn Manual such as Dieter Fleck, suggest that the Manual's greatest contribution to international humanitarian law is that it has proven that extant international humanitarian laws still apply to cyber warfare.[110]

---

[106] Ibid 58.

[107] National Cyber Security Centre 'Reckless campaign of cyber attacks by Russian military intelligence service exposed' available at *https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed* accessed 7 October 2019.

[108] Ibid.

[109] Cordula Droege 'Get off my Cloud: Cyber warfare, international humanitarian law, and the protection of civilians' *International Review of the Red Cross* accessed 7 November 2019 available at *https://www.cambridge.org/core/services/aop-cambridge-core/content/view/72114EF6E71757FAB2B37E7DE918B2BB/S1816383113000246a.pdf/get_off_my_cloud_cyber_warfare_international_humanitarian_law_and_the_protection_of_civilians.pdf* at 541.

[110] Nam Khoa Nguyen 'The international humanitarian law implications of the Tallinn Manual' available at *https://www.e-ir.info/2014/02/12/the-international-humanitarian-law-implications-of-the-tallinn-manual/* accessed on 7 November 2019.

The factors (discussed in the Manual) that victim states of cyberattacks should consider when making use of force assessments have also been included in books on the subject,[111] which I submit denotes further acceptance among scholars.

The most commonly identified criticism of The Manual can be summarized by the following quote by Nam Khoa Nguyen, 'Despite not being the panacea for international law on cyber warfare, the Manual still provides a foundation to assess the legality of cyber warfare in international and non-international armed conflict.'[112] This is because despite the acknowledgment that the Manual does provide a solid foundation regarding the applicability of international law to cyber warfare, the most common critique is that the Manual does not answer *all* the questions inherent in cyber warfare.[113]

Mary O'Connell for example, claimed that there still exists the potential for miscalculation in the interpreting of the *jus ad bellum*.[114] Some of the other criticisms of the Tallinn Manual are: that it does not specify what constitutes a cyberweapon, nor does it attempt to make any definitive conclusions on them;[115] that the composition of the 'Experts' which compiled the Manual reflected a geographic bias;[116] the experts were unable to reach consensus on a number of issues;[117][118] that the Tallinn Manual referenced only the military manuals of Canada, Germany, the UK and the US;[119] and that the Manual does not only ground its validity in legal sources, but also seeks to rely on the specific position and reputation of the experts in order to add credibility to the Manual.[120]

I submit that these critiques are not fatal to the Tallinn Manual's credibility and its use in this dissertation. This is because many of the omissions that attracted criticism

[111] Oxford Handbook on the use of force in international law chapter 52. Cyber threats and international law chapter 10.
[112] Nam Khoa Nguyen Op Cit note 110.
[113] Ibid.
[114] Ibid.
[115] Ibid.
[116] Oliver Kessler and Wouter G. Werner 'Expertise, uncertainty, and international law' (2013) *Leiden Journal of International law* at 805.
[117] Nam Khoa Nguyen Op Cit note 110.
[118] Examples are finding consensus on the definition of "attacks" and a lack of consensus on what constituted 'war-sustaining' military objectives.
[119] Oliver Kessler and Wouter G. Werner Op Cit note 116 at 803.
[120] Ibid at 804.

related to cyber warfare and its relationship to international humanitarian law,[121] and not to the scope of this dissertation which is whether cyberattacks can be an armed attack or a use of force under article 2(4) of the UN Charter. Finally, the fact that Dr. Cordula Droege (who represented the ICRC during the drafting of the Manual) described the Manual as a 'useful compilation of rules with commentary reflecting the different views on some of the thorny issues raised by this new technology',[122] and the fact that the Manual was peer reviewed prior to publication serves to preserve its credibility.

CONCLUSION

The creation of the UN Charter ushered in an era whereby a state could only legally use force in self defence if that state was the victim of an armed attack. Building on the previous chapter which argued that cyberweapons were weapons and could cause damage similar to traditional weapons, this chapter aimed to prove that cyberattacks could constitute an armed attack. This chapter relied on the Tallinn Manual where 20 international law experts concurred, basing their opinion on general principles of international law and ICJ decisions.

According to the experts, international law does not specify, and therefore does not limit which weapons may be utilized for a use of force. Additionally, much emphasis was placed on the *scale and effects* of the cyberattack, a threshold which can be met with cyberweapons and cyberattacks. It is therefore evident that cyberattacks are capable of being armed attacks.

Having established that cyberattacks can be an armed attack or 'most grave' use of force, the next chapter will discuss whether cyberattacks can be a 'less grave' use of force.

[121] The issues that recurred most related to issues regarding the principle of distinction and proportionality.
[122] Cordula Droege Op Cit note 109 at 541.

CHAPTER FOUR: ARE CYBERATTACKS A USE OF FORCE?

Although the previous section found that cyberattacks could be an armed attacked ('most grave' form of the use of force) and therefore automatically satisfy the requirement to be a 'less grave' use of force, I do not think that this is where the investigation should conclude. This is because the majority of cyberattacks either do not rise to the *scale and effects* to constitute an armed attack or they are cyberattacks which have non-violent effects.

Additionally, states are also actively curating their cyberattacks to fall below this threshold. An example of this is the United States which retaliated against Iran shooting its drone down with a cyberattack which was designed to stay 'well below the threshold of war'.[123] I submit that cyberattacks falling below this threshold, or cyberattacks with non-violent consequences are also capable of contravening article 2(4) of the UN Charter.

This chapter therefore has multiple objectives. The first is to argue that the prohibition of 'force' within article 2(4) of the Charter includes the use of cyberattacks. I will argue that the provision was intended to prohibit interstate conflict, and that the term 'force' was used in order to avoid the exploitation of any loopholes that were common prior to the Second World War. I submit that the term 'force' is not to be interpreted narrowly, but to be interpreted broadly so as to include cyberattacks.

Secondly, even if the reader does not accept my first argument for a broad interpretation of 'force' extending to include cyberattacks, I will argue that force is a term capable of evolving over time to include the use of cyberattacks. I will provide evidence that the concept has in fact evolved over time.

My final argument in this chapter relates to the non-violent cyberattacks or those falling below the threshold of an armed attack. Due to the lack of state practice and ICJ jurisprudence on cyberattacks, this chapter will identify cyberattacks which are

[123] Marc Schack 'Did the US stay "well below the threshold of war" with its June cyberattack on Iran?' available at *https://www.ejiltalk.org/did-the-us-stay-well-below-the-threshold-of-war-with-its-june-cyberattack-on-iran/* accessed on 7 October 2019.

'less grave' uses of force and factors victim states should consider when making use of force assessments.

SECTION A: PRE-CHARTER ATTEMPTS TO REDUCE FORCE

This section will argue that the prohibition of 'force' includes the use of cyberattacks. This section will discuss the pre-charter attempts to limit force, the drafting of article 2(4) and will interpret various provisions in the UN Charter in order to argue that the prohibition of 'force' includes the use of cyberattacks.

Although the UN Charter prohibits force, there remains no treaty definition of what force entails. In such situations, reference is made to articles 31 and 32 of the Vienna Convention on the Law of Treaties which, despite coming into force after the UN Charter, is a codification of customary international law.[124] This has been confirmed by the ICJ in the *Case Concerning the Pulp Mills on the River Uruguay* case,[125] where the Court held that the Vienna Convention on the Law of Treaties reflected customary international law and could be used to interpret treaties which came into force before the Vienna Convention.[126]

Article 31 states that:

> (1) A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose.

Additionally, article 32 states that:

> Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31:
>
> (a) Leaves the meaning ambiguous or obscure; or
> (b) Leads to a result which is manifestly absurd or unreasonable.

---

[124] TW Bennet and J Strug *Introduction to International Law* (2013) at 128.
[125] (Argentina v. Uruguay) (2010) Rep 14 ICJ.
[126] Para 65-66.

(a) Attempts to reduce force

Historically, the use of force by states was allowed, provided it was for a just cause.[127] War was justifiable, if that war was waged against the authority of a sovereign (the state), a prior wrong had been committed, and the belligerent intended to advance good and avoid evil.[128]

The historic concept of war was best described by Francisco Suarez who described war in these terms:

> An external contest of arms which is incompatible with external peace is properly called war, when carried out between two sovereign princes or between two states. When however, it is a contest between a prince and his own state, or between citizens and their state, it is termed sedition. When it is between private individuals it is called a quarrel or duel. The difference between these various kinds of contests appears to be material rather than formal.[129]

The position whereby war could only be waged for a just cause changed in the 19th century as this requirement was ignored by states and they took up arms freely to enforce their interests.[130] This created uncertainty about the legality of warfare and sparked a debate as to when war could be considered to have begun, with the objective view asserting that a situation of war had been created by the mere fact of an armed conflict; while the subjective view held that an accompanying *animus belligerendi* was also necessary.[131] This was settled, whereby intention was communicated by a declaration of war, however, these declarations were in practice no more than a formality.[132]

From the above, one could say that a state of war existed when there had been a declaration of war, an act of force had been committed *animo belligerendi* under the

---

[127] TW Bennet and J Strug Op Cit Note 124 at 319.
[128] Ibid.
[129] Jens David Ohlin, Kevin Govern, and Claire Finkelstein *Cyberwar: Law and Ethics for Virtual Conflicts* (2015) at 3.
[130] TW Bennet and J Strug Op Cit note 124 at 319.
[131] Ibid at 320.
[132] Ibid.

authority of a state, or a belligerent chose to regard an act as warlike.[133] The establishment of the status of war had a positive effect because once war was established, the parties were governed by humanitarian laws.[134]

The Hague Peace Conferences of 1899 and 1907 introduced the first attempts to restrict the recourse to war.[135] Convention (I) aimed to resolve disputes through peaceful measures before states turned to war.[136] Contracting parties were 'animated by a strong desire to concert for the maintenance of the general peace' and 'resolved to second by their best efforts the friendly settlement of international disputes'.[137] Convention (III) related to the Opening of Hostilities, contracting parties agreed to not commence hostilities between them without previous and explicit warnings, in the form of either a declaration of war containing reasons for the commencement of hostilities, or an ultimatum with a conditional declaration of war.[138]

Despite the abovementioned and other conventions, the outbreak of World War I could not be prevented. In the aftermath of the First World War, a popular opinion emerged which held that belligerents had accidently slipped into a state of war,[139] and that had there been a forum available to discuss grievances and misunderstandings, the War could have been avoided. This led to a renewed political commitment to restrict warfare with the establishment of the League of Nations in 1919 which sought to 'promote international co-operation and to achieve international peace and security by the acceptance not to resort to war'.[140] Article 10 of the Covenant seemed to prohibit force when it stated:

> The members of the league undertake to preserve as against external aggression the territorial integrity and existing political independence of all members of the League. In the case of any such aggression or in case of threat of danger of such aggression the Council shall advise upon the means by which the obligation shall be fulfilled.

---

[133] Ibid.
[134] Ibid.
[135] Marc Weller *The Oxford Handbook of the Use of Force in International Law* (2015) at 466.
[136] Ibid.
[137] Ibid.
[138] Ibid at 467.
[139] Ibid.
[140] Covenant of the League of Nations, 1919 at Preamble.

However, this provision was not a prohibition against force and the subsequent articles make it clear that article 10 is merely a duty to submit their disputes to consultation, arbitration, judicial settlement or inquiry by the Council of the League of Nations.[141] Evidence of this can be found in article 12, which required states to submit their disputes to either arbitration, judicial settlement or inquiry by the League Council, and they were to wait three months after the decision before resorting to war. This three month cooling-off period was intended to prevent states from resorting to war.

In addition to the Covenant of the League of Nations, there were several other attempts made to prevent war. The Geneva Protocol for the Pacific Settlement of International Disputes is considered as the first attempt at imposing compulsory dispute settlement. However, this Protocol failed to materialize.[142] The Locarno Treaty of Mutual Guarantee also attempted to regulate the use of force.[143] Here, Belgium, Germany and France agreed that they would 'in no case attack or invade each other'.[144]

However, the most significant attempt outside the Covenant to regulate the use of force was the Kellogg-Briand Pact or the Pact of Paris in 1928, whereby 63 states (virtually the entire international community at the time) declared that they would 'condemn recourse to war for the solution of international controversies, and renounce it as an instrument of national policy in their relations with one another.'[145] Article 2 states that conflict should only be solved through pacific means. The Pact of Paris can be seen as the first widely accepted denunciation of war.[146]

The League of Nations and the Pact of Paris were unable to prevent the outbreak of the Second World War, and the prohibitions on the use of force contained in the aforementioned agreements depended on how parties chose to interpret the term 'war'.[147] Although the Pact of Paris specifically outlawed war, it did not outlaw force in general. States who wanted to shirk their treaty obligations interpreted the term

[141] Marc Weller Op Cit Note 135 at 467.
[142] Ibid at 468.
[143] Ibid.
[144] Ibid.
[145] Article 1.
[146] Marc Weller Op Cit Note 135 at 468.
[147] TW Bennet and J Strug Op Cit note 124 at 322.

restrictively, or they would resort to war without formal declarations of war.[148] Examples of these evasive measures were provided by Japan who referred to their invasion of China as an 'incident', Italy's annexation of Abyssinia was labelled an 'expedition' by Mussolini, and Germany's 'Anschluss' (joining) of Austria in 1938 led to the outbreak of WWII.[149] Other times, states such as Japan, Germany and Italy simply chose to withdraw from the League of Nations altogether.[150]

The failure of the League did not deter allied states from pursuing an international system of collective security, and this ultimately led to the creation of the Charter of the United Nations. The UN Charter retained certain principles of the Covenant of the League of Nations such as aiming for collective security, but made no allowances for members to withdraw from the UN.[151] Furthermore, the Charter made it clear that war would no longer be tolerated in its Preamble, and article 2(4) of the Charter contained an all-encompassing prohibition on the threat or use of force similar to article 10 of the League's Covenant. Article 2(4) states that:

> All members shall refrain in their international relations from the threat or the use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purpose of the United Nations.

By erasing 'war' or 'aggression' from article 2(4), the drafters of the Charter hoped to avoid the semantic controversies that plagued the League of Nations,[152] and the Charter only permitted unilateral force in self defence under article 51. Below, I will discuss the drafting of article 2(4) and refer to the *travaux preparatoires* of the UN Charter in order to decipher what the drafters of the Charter sought to include and exclude in the prohibition in article 2(4).

(b) The drafting of article 2(4)

At the San Francisco conference, there were several rounds of discussion regarding the formulation of what would become article 2(4) of the Charter, which sought to

[148] Ibid.
[149] Marc Weller Op Cit Note 135 at 469.
[150] TW Bennet and J Strug Op Cit note 124 at 322.
[151] Ibid at 322.
[152] Ibid at 323.

prohibit the use of force in as absolute terms as possible.[153] The allied powers wanted to make the independent use of armed force by any member of the UN unlawful, except in cases of self defence against aggression.[154]

During the negotiations, there were calls for an expanded prohibition of force in order to include other types of force other than armed force.[155] Brazil proposed prohibiting economic force, Ecuador proposed the prohibition of moral or physical force, and Iran demanded the inclusion of political force within the prohibition and wanted the provision to include the following:

> All the Members of the Organisation should refrain from intervening in their international relations, whether directly or indirectly, in the international affairs of the other States and from the threat or the use of force in any manner inconsistent with the Purposes of the Organisation.[156]

None of these proposals were adopted.

A second point of discussion at the Conference was the insertion of the prohibition of aggression into article 2(4) which was proposed by Brazil.[157] Brazil proposed that the following provision be added:

> All threats or acts of violence committed by any state to the detriment of any other state shall be considered as acts of aggression committed against all other members of the Organisation.[158]

Similar provisions were proposed by Ecuador, Bolivia and New Zealand, with the latter proposing a provision which advocated for the collective undertaking against aggression, which said: 'All members of the Organisation undertake collectively to resist every act of aggression against any member.' [159] These proposals referring to aggression were opposed by China, the US and the UK as they felt that it would narrow the scope of article 2(4).[160] According to these states, aggression would be better covered by the term 'threat to peace'. Although New Zealand's amendment

[153] Marc Weller Op Cit Note 135 at 470.
[154] Ibid.
[155] Ibid at 470.
[156] Ibid.
[157] Ibid.
[158] Ibid.
[159] Ibid
[160] Ibid.

received 26 votes in favour and 18 against, it was unable to be adopted because it failed to receive the two-thirds majority required to form part of article 2(4).[161]

A third point of discussion concerned the final part of the provision 'or in any other manner inconsistent with the Purposes of the United Nations'.[162] Several delegates were concerned that this could be interpreted in a way whereby states could decide on their own whether or not the use of force was prohibited.[163] Costa Rica proposed that it be deleted in order to ensure that the prohibition of the use of force was absolute.[164] Norway supported the omission and instead proposed an alternative text aimed at the explicit prohibition of the threat or use of force not authorised by the Security Council in order to achieve the objectives of the Organisation.[165] Brazil also expressed concerns about the possibility of the last sentence being interpreted as authorising unilateral force by states, claiming that such action was in accordance with the objectives of the Organisation.[166] It proposed an amendment which allowed for action 'being taken according to the procedures established by the Organisation and in accordance with its decisions'.[167]

All of these were opposed by the UK and the US on the basis that the wording had been carefully considered in order to preclude interference with the enforcement clauses of Chapter VII of the Charter. The US and the UK argued that the text of the draft was the 'most intelligible, forceful and economical language'.[168] The US Delegate confirmed that the intention of the authors of the original text was to state in the broadest terms, an absolute all-inclusive prohibition, and that 'or in any other manner' was designed to ensure that there would be 'no loopholes'.[169]

Finally, based on the proposals of numerous small states, the Conference resolved to add 'against the territorial integrity or political independence of any State' to article 2(4) which was intended to be an extra and specific guarantee for smaller states.[170]

---

[161] Ibid.
[162] Ibid at 471.
[163] Ibid.
[164] Ibid.
[165] Ibid.
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] Ibid.
[170] Ibid.

(c) Preliminary conclusions

Briefly, what can be deduced from this section is that article 2(4) of the Charter was the culmination of numerous efforts by states to prohibit and prevent interstate conflict.

The term 'force' was also not intended to have a singular fixed meaning, and this can be deduced from the fact that the inclusion of terms like 'aggression' in the prohibition were seen to narrow the scope of article 2(4), implying that the intention was for this provision to have a broader interpretation. Article 2(4) was not intended to include all types of force, as certain types of force were excluded from the prohibition. From this it can be deduced that outside of the excluded types of force, other types of force could form part of this prohibition. It is evident that the term 'force' was not intended to have a narrow interpretation, but was adopted to prevent states from exploiting linguistic loopholes in the law.

(d) Evolution of the concept of force

From the negotiating of article 2(4) and the history that preceded it, I submit that the prohibition was initially intended to apply to interstate military force, which was the type of force that was prevalent at the time. I further submit that based on the negotiations surrounding the drafting of the provision, article 2(4) was not intended to be interpreted narrowly to only include this kind of force. Article 2(4) was also not intended to be interpreted so broadly as to include all types of force, and evidence of this is the explicit exclusion of moral, physical, political and economic force. Finally, the ICJ in the *Dispute Concerning Navigational and Related Rights*[171] created a presumption that generic terms were always in the process of developing meanings and that, consequently such a meaning is capable of evolving over a long period of time.[172] I submit that 'force' is one such generic term that is capable of developing over a long period of time, and that it has evolved to include the use of cyberattacks. Below, I will provide numerous examples of the development of this concept to show that the term is not static, but is capable of evolution.

[171] (Costa Rica v Nicaragua) (2009) ICJ Rep 213.
[172] Para 63-64.

(d)(i) Concept of force

The first development to be discussed is the concept of 'force'. Although the UN Charter does not provide a definition of force, the concept was developed by the *Nicaragua* case which divided the concept of force into two categories: the 'most grave' use of force (those consisting of an armed attack)[173] and 'less grave' uses of force such as a mere frontier incident carried out by regular armed forces.[174]

(d)(ii) Where

Article 2(4) of the Charter prohibits the threat or use of force by Members in their *international relations*, thus excluding the use of force by members solely within their own state.[175]

This was developed by UNGA Resolution 1514, which sought to give effect to the right of self determination and prohibited the use of force *internally* against liberation movements and 'peoples' asserting their right to self determination. This resolution stated that:

> All armed action or repressive measures of all kinds directed against dependent peoples shall cease in order to enable them to exercise peacefully and freely their right to complete independence, and the integrity of their national territory shall be respected.

This was repeated in UNGA Resolution 2625 which said:

> Every state has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self determination of that right to self determination and freedom and independence.

(d)(iii) Who

Article 2(4) prohibits the threat or use of force by Members, which are states. I have submitted above that this referred to a state's military forces.

---

[173] *Military and Paramilitary Activities in and Against Nicaragua* Op Cit note 14 Para 191.
[174] Ibid para 195.
[175] Bruno Simma, Daniel Erasmus-Khan, George Nolte, Andreas Paulus *The Charter of the United Nations: A Commentary* 3 ed (2012) at 214.

The Declaration of Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations in 1970, along with the *Nicaragua* case in 1986 developed the concept to show that force could be used by non-state actors such as irregular forces, armed band or mercenaries.

The resolution, which was relied on by the Court in *Nicaragua,* confirmed the following principles:

- Every state has the duty to refrain from organising or encouraging the organisation of irregular forces or armed bands, including mercenaries, for incursion into the territory of another state;[176] and
- Every state has a duty to refrain from instigating, assisting or participating in acts of civil strife or terrorist acts in another state or acquiescing in organised activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[177]

Finally, article 8 of the International Law Commission's Draft Articles on State Responsibility allowed for the conduct of a non-state actor to be attributable to a state if they acting at the behest of another state. This provision states that:

> The conduct of a person or group of persons shall be considered an act of State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that state carrying out the conduct.

(d)(iv) How

The lack of a definition of 'force' in the Charter creates ambiguity as to *how* force is prohibited. I submitted in the section above that this initially referred to military force and traditional weapons as this is what was available and conceivable at the time.

[176] *Military and Paramilitary Activities in and Against Nicaragua* Op Cit note 14 para 191.
[177] Ibid.

The *Legality of the Use of Nuclear Weapons* case stated that article 2(4) does not specify the type of weaponry required to constitute a use of force.[178] Therefore, this prohibition extends to weapons not available at the time of the adoption of the Charter such as chemical and biological weapons.[179] This interpretation means that weapons and methods of force not envisaged at the adoption of the Charter could fall within this prohibition, such as cyberweapons and the use of cyberattacks.

(e) UN Charter interpretation

The overall aim of international law is to reduce the levels of violence between states,[180] and in the aftermath of the Second World War, the UN Charter, specifically article 2(4), is tasked with maintaining international peace and security. This section will refer to various provisions in the UN Charter in order to support my assertion that article 2(4) was intended to prohibit interstate conflict, and not specifically armed conflict, which would also support the argument that cyberattacks are a use of force.

(e)(i) Preamble

When turning to the Preamble, there are numerous relevant provisions to support my assertion. The Preamble of the Charter declares that the United Nations is determined to:

> Save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind and,
>
> …
>
> To establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained,
>
> …
>
> To Practice tolerance and live together in peace with one another as good neighbours, and
>
> To unite our strength to maintain international peace and security.

[178] *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* (1996) ICJ para 39.
[179] Michael N. Schmidt Op Cit note 80 at 54.
[180] Nigel D. White *Advanced Introduction to International Conflict and Security Law* (2014) at 1.

The preamble's intention is to highlight some of the motives of the founders of the UN and to serve as an interpretive guideline for the provisions of the Charter.[181] The wording 'to save succeeding generations from the scourge of war, which twice in our lifetime has brought about untold sorrow of mankind' was accepted by all delegates and was meant to stress not only that the creation of the Organization is a response to the two World Wars, but it also indicated the intention of Member States to suppress war.[182]

From the above it is evident that the aims of the Charter were to prevent war or interstate conflict (the likes of which had been prominent at the time), but to also create and maintain conditions where states do not need to engage in conflict.

To 'practice tolerance and live in peace with one another as good neighbours' is another provision of the Preamble. Although there has been some debate as to whether 'neighbours' referred to the narrow geographical sense, or whether it was to have a more far reaching meaning,[183] I submit that the provision's inclusion in Resolution 2625 supports the latter. I submit the wording in the resolution is directed to members of the international community as a whole and calls on states to adhere to the Principles of the Charter in order to achieve and maintain international peace and security. A narrow interpretation whereby states are only to be good neighbours to their immediate neighbour is contrary to the aims of the Charter and of this resolution.

(e)(ii) Article 1

The first chapter of the Charter contains article 1 and 2, which are the Purposes and Principles of the Charter, and these are intended to provide a guide for the conduct of the UN in a fairly flexible manner.[184] These Principles and Purposes are intended to supplement the Preamble which expresses the ideas which guided the state parties when establishing the UN.[185]

[181] Bruno Simma, Daniel Erasmus-Khan, George Nolte, Andreas Paulus Op Cit note 175 at 105.
[182] Ibid at 103.
[183] Ibid at 105.
[184] Ibid at 108.
[185] Ibid.

Article 1 of the Charter which addresses the Purposes of the Charter, states that the purposes of the UN Charter are:

1. To maintain international peace and security, and to that end: to take effective collective measures for the removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;
2. To develop friendly relations among nations based on principle of equal rights and self determination of peoples, and to take other appropriate measures to strengthen universal peace;

   …
4. To be a centre for harmonising the actions of nations in the attainment of these common ends.

It is a matter of controversy as to whether the Purposes contained in article 1 are intended to be legally binding. However, certain commentators assert that article 1(1) and (2) are considered principles binding under customary international law regarding the prohibition of aggression, the prohibition of other breaches of peace and the obligation to settle disputes by peaceful means.[186]

Although article 1 does not indicate how a possible conflict between the different purposes might be resolved, some commentators assert that it can only be achieved by giving priority to the lasting preservation of peace, which has been described as 'the purpose of all purposes'.[187] In the *Certain Expenses* case, the ICJ stated that 'the primary place ascribed to international peace and security is natural, since the fulfilment of the other purposes will be dependent upon the attainment of that basic condition'.[188] This supports my interpretation that article 2(4) cannot narrowly be interpreted to prohibit only armed attacks because the main aim of the Charter is to preserve international peace. Such a narrow interpretation which allows states to

[186] Ibid.
[187] Ibid at 109.
[188] *Certain Expenses of the United Nations* (1962) ICJ para 168.

engage in other forms of conflicts such as cyberwarfare is contrary to the aims of the Charter.

The term 'international peace and security' is used frequently throughout the Charter. The Preamble and article 1(1), (2) and (3) indicate that the concept of peace consists of more than the absence of war.[189] According to some commentators, these provisions refer to an evolutionary development in the state of international relations which is meant to lead to the reduction of these issues likely to cause war.[190] If these provisions are intended to reduce issues likely to cause war, then I submit that this would include cyberattacks being included in the prohibition, because excluding them and permitting their use may escalate to a conventional war, which would be contrary to the aims of the Charter.

Article 1(1) refers to the maintenance of international peace and security as the overarching purpose of the UN, whereas the suppression of aggression is only referred to as one objective to be achieved through measures of collective security.[191] From this, it becomes evident that international peace and security cannot only be endangered by acts of aggression, but also by any other threat to the peace. Additionally, it means that the suppression of aggression as an objective of the UN is subordinate to the maintenance of international peace and security.[192] Again, this supports the interpretation that article 2(4) is intended to prohibit interstate conflict in numerous ways including cyberattacks, it is not only intended to prohibit military conflict.

(e)(iii) Article 2

Article 2 of the Charter requires Members to pursue the purpose of article 1 and to act in accordance with the principles that will be discussed below.

Article 2 of the Charter states that:

> The Organization and its Members, in pursuit of the Purpose stated in article 1, shall act in accordance with the following (relevant) Principles:

[189] Bruno Simma, Daniel Erasmus-Khan, George Nolte, Andreas Paulus OP Cit note 175 at 110.
[190] Ibid.
[191] Ibid.
[192] Ibid at 112.

1. The Organization is based on the principle of the sovereign equality of all its Members;
2. All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfil in good faith the obligations assumed by them in accordance with the present Charter; and
3. All members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice are not endangered.

According to the Chairman of the Sub-Committee of the San Francisco Conference, the Principles contained in article 2 of the Charter indicate the *raison d'etre* of the Organization.[193] These Principles express the basic rules to be followed in order to achieve the purposes of article 1 and the intentions of the Preamble.[194] Article 2 requires Members to act in pursuit of the Purposes contained in article 1. According to some commentators, following the Principles in a schematic way is not sufficient. Rather, the Principles must be observed in pursuit of, or with the goal of achieving the Purposes of article 1.[195] From this it is evident that there are no specific actions states must take to achieve the purposes of article 1. Instead, this requires states' general behaviour to be in pursuant to the goals in article 1. I submit that permitting the use of cyberattacks would be contrary to the principles of the Charter.

(e)(iv) Preliminary conclusions

The overarching aim of the United Nations is to maintain international peace and security, which is why this has been described as the 'purpose of all purposes'. Although there is support for 'force' in article 2(4) referring to military force, I submit that is too limited an interpretation and should include methods of force not expressly rejected in the negotiating process. For the purpose of this dissertation, I submit that the correct interpretation of article 2(4) should prohibit the use of cyberattacks. Having looked at the history building up to the drafting of the provision, I have showed that delegates had opportunities to limit the meaning of the

[193] Ibid at 127.
[194] Ibid.
[195] Ibid.

provision, but instead opted for the current articulation which is broader so as to not limit the scope of the provision and to avoid any possible 'loopholes'.

I submit that a narrow interpretation of this provision which excludes the use of cyberattacks from its scope would be contrary to the aims and Purposes of the Charter, which, according to article 32(b) of the Vienna Convention on the Law of Treaties, would lead to a result which is manifestly absurd or unreasonable. This is because a narrow interpretation of article 2(4) which excludes cyberattacks would promote the use of cyberattacks between states and could escalate to an international armed conflict, which is one of the things the Charter aims to prevent. This outcome would directly contradict the main purpose of the Charter which is to maintain international peace and security, and not to prevent armed conflict specifically. When you factor the previous chapter where I concluded that cyberweapons were weapons, it would be absurd to conclude that states are permitted to use cyberattacks against one another when article 2(4) prohibits them from using other kinds of weapons against each other.

The potential for cyberattacks to destabilize international peace and security was echoed by a UN-convened panel of governmental experts who noted that 'existing and potential threats in the sphere of information security are among the most serious challenges of the twenty first century… Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.'[196]

By continuing to employ cyberattacks against one another, states are not only acting against the aims the UN is seeking to achieve, but they are directly contravening their obligations under article 2(4) of the UN Charter.

To borrow reasoning from the *Prevention of Genocide* case:[197]

> It would be paradoxical if States were thus under an obligation to prevent, so far as within their power, commission of genocide by persons over whom they have a certain influence, but were not forbidden to commit such acts through their own organs, or persons over whom they have such firm control

[196] Matthew C. Waxman Op Cit note 73 at 424.
[197] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro) (2007) ICJ.

> that their conduct is attributable to the State concerned under international law. In short, the obligation to prevent genocide necessarily implies the prohibition of the commission of genocide.[198]

I submit that the same rationale can be transposed to states in the UN who undertake to achieve and maintain international peace and security. I submit that it would be paradoxical for states to commit to the pursuit of 'the purpose of all purposes' which is maintaining international peace and security, while still being permitted to conduct cyberattacks against other states.

SECTION B: ECONOMIC FORCE

During the drafting of article 2(4), one of the forms of force which was expressly excluded from falling under article 2(4) was economic force. As one of the targets of a cyberattack could be a state's financial system, it is therefore imperative to ascertain what economic force entails and whether a cyberattack which targets a state's financial infrastructure falls within this exclusion.

Economic force is a difficult term to define with precision, but it has been used to describe conduct ranging from belligerent blockades and the strategic bombing of factory infrastructure;[199] to decentralised economic countermeasures during peacetime such as trade embargoes; boycotts by citizens of one state against the products of another state; to collective sanctions imposed by the UN Security Council.[200]

Economic force is not a new form of force and can be traced back to the Peloponnesian War between Athens and Sparta (431-404 BC) where the Athenians imposed trade sanctions on Megara, and this was considered an act of war by the Spartans.[201] Economic force continued to feature in conflict between nations and, in the 17th century, Grotius dealt extensively with the law regulating the classical methods of economic force such as naval blockades and contraband.[202] The numerous blockades, sieges and restrictions of trade throughout history attest to the

---

[198] Ibid Para 166.
[199] Frauke Lachenmann and Rudiger Wolfrum *The law of armed conflict and the use of force: the Max Planck Encyclopaedia of Public International Law* (2017) at 344.
[200] Ibid.
[201] Ibid.
[202] Ibid at 345.

fact that economic force is a supplement, if not an alternative to military engagement.[203]

Economic force can broadly fall within two categories which will be discussed below: economic force during armed conflict and economic force during peacetime.

(a) Economic force during armed conflict

(a)(i) Economic force using armed force

The clearest example of economic force during an armed conflict is a naval blockade, and this refers to not only the blockade, but to the visit and search of vessels, their subsequent capture, and the interception of contraband.[204]

A naval blockade of enemy ports intends to cut off all maritime communication and in particular, all maritime trade between the target state and the rest of the world with the intention of putting a strain on a state's resources.[205] Notable blockades occurred during the Napoleonic Wars, the American Civil Wars and the Two World Wars.[206]

'Visit and Searches' also operate as a more specific means of economic force than a general blockade, and refers to the capture and condemnation as prize of enemy merchant ships and their cargo, but can also lead to the capture of neutral merchant vessels or the confiscation of their cargo if these are carrying cargo for an enemy state.[207] A notable example occurred during the 1999 NATO campaign in Kosovo, where NATO maintained that it could exercise 'visit and searches' in order to restrict the flow of strategic commodities into the Federal Republic of Yugoslavia.[208]

'Contraband' refers to cargo aboard neutral merchant vessels bound for territory controlled by the enemy and susceptible for use in armed conflict.[209] While private merchants from neutral states may not be prohibited by belligerents from trading with an enemy material or war-related items, they risk having their ships or cargo confiscated if they engage in such trade.[210]

---

[203] Ibid.
[204] Ibid.
[205] Ibid.
[206] Ibid.
[207] Ibid at 346.
[208] Ibid.
[209] Ibid.
[210] Ibid at 347.

Although this section has focussed on naval blockades to illustrate examples of forceful methods of economic force, it is of course possible to implement blockades by the use of land and air forces.[211] An example is the blockade of Berlin from 1948 to 1949.

(a)(ii) Economic force not involving armed force

Beyond blockades, there are general measures of economic force taken during an armed conflict which are not linked to a military operation or may not require the use of armed force at all.[212] These forms of economic force take the form of domestic legislation or administrative acts.[213] These measures will primarily be directed at persons, property and conduct within the jurisdiction of the legislating state, and will typically prohibit any trading with the enemy.[214] However, these measures can go beyond that and may also freeze all enemy funds and assets in the legislating state, and that state may also impose specific trade restrictions such as the prohibition of exports or the reduction of export quotas.[215] Laws prohibiting trade with the enemy were prominent during the Two World Wars, with the UK's Trading with the Enemy Acts of 1914 and 1939 offering a good example of this connection.[216] These acts primarily provided for the application of a territorial test, according to which people within the UK jurisdiction were forbidden to trade with anyone residing 'beyond the line of war'.[217] This prohibition applied irrespective of nationality, as individuals and companies in enemy territory were deemed to be enemy aliens by the operation of the law.[218]

Other administrative or legislative measures to compliment military force include the freezing of enemy assets in the territory of the acting state.[219] Finally, imposing embargoes, which refer to the prohibition of imports or exports to an enemy state is

[211] Ibid.
[212] Ibid at 348.
[213] Ibid.
[214] Ibid.
[215] Ibid.
[216] Ibid.
[217] Ibid.
[218] Ibid.
[219] Ibid.

also a common method of economic force even if it is not supported by a blockade.[220]

(b) Economic Force in peacetime

The use of economic force is not limited to times of armed conflict but can also be relied on during times of peace. This is because there are certain measures taken during times of peace that may resemble traditional economic force to such an extent that it is fair to say that economic force – in the form of economic coercion – is not merely limited to being supplementary to armed conflict, but can be an alternative to armed conflict.[221] This development is in part a result of the creation of the UN Charter in two separate but interconnected ways.

The first is the prohibition of the use of force contained in article 2(4) of the Charter, which has put a strain on the traditional distinction between wartime and peacetime.[222] States are reluctant to take action which may violate this provision, and when they do wish to apply pressure on other states, they are likely to employ measures which do not amount to armed force.[223]

The second way in which the UN Charter impacted economic force is that it institutionalized it and attempted to incorporate it within the framework of Chapter VII.[224] Under article 41, the Security Council may order the imposition of measures including the 'complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication.

Under article 42, the Security Council may take action 'by air, sea, or land forces', including 'demonstrations and blockade' in order to maintain international peace and security. Both these types of measures allude to the use of economic force.

The rest of this section will be divided into institutionalized economic force which is authorised by the Security Council and decentralized economic force which refers to the unilateral use of economic force by states.

---

[220] Ibid.
[221] Ibid at 349.
[222] Ibid.
[223] Ibid.
[224] Ibid at 350.

(b)(i) Institutionalized Economic Force

Institutionalized economic force takes the form of collective measures imposed or authorised by the Security Council.[225] Article 41 of the Charter allows for the Security Council to use non-armed forms of force in order to maintain international peace and security. Acting under this provision, the Security Council has imposed embargoes on states on numerous occasions, some of which have been so comprehensive that they applied to all trade between the target state and all other states.[226]

The Security Council has also resorted to financial sanctions on numerous occasions. Financial sanctions require states to freeze all financial assets of the target that are located within its jurisdiction, and these may be imposed by a state, personally against the leaders of a state, individuals or other entities that constitute a threat to international peace and security.[227]

The Security Council has even relied on article 42 to authorise the use of force in order to enforce and imposed a trade embargo.[228] In such circumstances where the Security Council is authorising force in order to enforce a trade embargo, it is effectively imposing a blockade.[229]

(b)(ii) Decentralized Economic Force

Decentralized peacetime measures which may qualify as economic force are those measures taken unilaterally by states that target the economy of another state with the intention of applying pressure to bring about change in the conduct of the target state.[230] This includes the economic embargoes or boycotts, the reduction or withdrawal of economic aid, restrictions in trade such as the reduction in quotas, and the freezing of the state's financial assets.[231]

The legality of these measures will depend on the circumstances and on the particular obligations in force between the states in question, and they may qualify as a)

---

[225] Ibid.
[226] Ibid.
[227] Ibid.
[228] Ibid at 351.
[229] Ibid.
[230] Ibid.
[231] Ibid.

measures of retorsion, if they are lawful but unfriendly;[232] b) as countermeasures, if they are in breach of international obligations, but their wrongfulness is precluded because it was taken in response to a particular breach; or c) as breaches of international obligations, engaging the international responsibility of the state resorting to them.[233]

The ICJ in *Nicaragua* found that a "state is not bound to continue particular trade relations longer than it sees fit to do so, in the absence of a treaty commitment or other specific legal obligation."[234] Therefore, in the absence of a legal obligation to engage in trade with another state, a general trade embargo may be a lawful measure.

Numerous examples of decentralized measures of economic force can be referred to and these measures are usually justified by the acting states as being a response to a perceived violation on the part of the target state.[235] Examples are the Arab oil boycott in the 1970s against states supporting Israel,[236] the measures against the USSR for its intervention in Afghanistan in the 1980s,[237] as well as the US response to the Iranian violation of diplomatic law in the hostage crisis.[238]

(c) Cyberattack and economic damage: conclusions

The aim of this section was to ascertain whether cyberattacks targeting the economy or financial system of a state fall within the concept of economic force. I submit that cyberattacks causing economic harm do not fall within the concept of economic force as outlined above, and therefore can constitute a use of force. I base this assertion on the material differences between the two which I will outline below.

The first difference between cyberattacks and economic force such as embargoes is that economic force is external and gradual while cyberattacks are internal and swift.[239] The oil embargo of 1973 lasted for almost six months and the stock market crash only occurred in the second half of the embargo.[240] Although the embargo was

[232] Ibid
[233] Ibid.
[234] *Military and Paramilitary Activities in and Against Nicaragua* Op Cit note 14 para 276
[235] Frauke Lachenmann and Rudiger Wolfrum Op Cit note 199 at 352.
[236] Ibid.
[237] Ibid.
[238] Ibid.
[239] Georg Kerschischnig Op Cit note 24 at 132.
[240] Ibid.

probably a decisive factor, it was not the only factor for the crash.[241] Cyberattacks could disable targets such as financial markets in a way that neither kinetic force, nor political or economic sanctions could.[242]

Secondly, cyberattacks are more likely to last for a short period of time and produce immediate direct results such as the destruction of data, while economic force takes longer and its consequences would be indirect.[243]

Thirdly, economic force is based on the external influencing of market forces.[244] A cyberattack on the other hand involves intrusive actions in the target state's sphere such as the hacking of its systems and introduces a sovereignty-encroaching element that influences the market internally.[245]

Fourthly, a cyberattack can also be more accurately targeted, with the potential to cause damage to both intangible and tangible property.[246]

Finally, cyberattacks causing economic harm resemble more of an attack by conventional weapons than any of the forms of economic force mentioned above.[247] Cyberattacks are also generally intrusive, and also contravene the principle of non-intervention. Economic force still appears to respect the territorial sovereignty of states and fails to cross the threshold of violating the principle of non-intervention.

If on one end of the spectrum there is economic force, and on the other end there are attacks by traditional weapons on physical infrastructure causing economic harm (such as the bombing of the stock exchange for example), then I submit that cyberattacks do not resemble economic force at all and would fall closer on the spectrum to a conventional attack. Therefore, I submit that cyberattacks causing economic damage do not fall within the excluded concept of economic force and are therefore able to be classified as a use of force.

---

[241] Ibid.
[242] Ibid.
[243] Ibid.
[244] Ibid.
[245] Ibid.
[246] Ibid.
[247] Ibid.

SECTION C: CYBERATTACKS AS A USE OF FORCE

As has been stated numerous times before, not all cyberattacks have violent consequences or rise to the threshold of an armed attack. I submit that the non-violent cyberattacks and those falling below the threshold of an armed attack are also capable of contravening article 2(4) of the UN Charter. It is also important to establish whether a cyberattack is a 'most grave' use of force, a 'less grave' use of force or neither as this will determine what responses the victim state may legally pursue.

The submission that non-violent cyberattacks and those falling below the threshold of an armed attack are capable of contravening article 2(4) is also supported by the Tallinn Manual which outlined numerous factors that states could consider when making a use of force assessment. The most important conclusion that can be drawn from the Tallinn Manual is that these cyberattacks *can* be uses of force, even though much would depend on the surrounding circumstances. This section will rely on the Tallinn Manual, where the group of experts attempted to address the issue of non-violent cyberattacks, or cyberattacks which fall below the threshold of an armed attack.

The experts identified numerous factors involved in a cyberattack to be considered by victim states when they make a use of force assessment. Their goal was to identify cyberattacks that were similar to other attacks which the international community would describe as a use of force.[248] Their approach seems to suggest that states would place significant weight on the following factors when deciding whether a cyberattack is a use of force. According to the international group of experts, states would look at the following factors:

(a) Severity: Subject to a *de minimus* rule, consequences involving physical harm to individuals or property will, in and of themselves, qualify as a use of force. Those causing mere inconvenience will never do so.[249] Between these two extremes, the more consequences that a cyberattack causes on critical national interests, the more they will be considered as a use of force.[250]

[248] Michael N. Schmidt Op Cit note 80 at 49.
[249] Ibid.
[250] Ibid.

Additionally, the scope, duration, and density of the consequences will also have a bearing on the appraisal of their severity.[251] According to the experts, severity is self evident and the most important factor in this analysis.

(b) Immediacy: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to forestall their harmful effects.[252] States are more concerned about immediate consequences than they are about those that are delayed or that will develop slowly over time.[253]

(c) Directness: The greater the attenuation between the initial act and its consequences, the less likely states will be to find an actor to be in violation of the prohibition of the use of force.[254] Directness differs from the immediacy factor in that immediacy focusses on the temporal aspects of the consequences, while directness examines the chain of causation.[255] Cyberattacks where the cause and effects are clearly linked are more likely to be considered as uses of force.

(d) Invasiveness: This refers to the degree to which the cyberattack intrudes on the target states or its cyber systems contrary to the interests of the state.[256] The general rule is that the more secure a targeted cyber system is, the greater the concern as to its penetration.[257] For example, penetrating a military system is more invasive than penetrating civilian systems.

(e) Measurability of effects: This factor stems from the willingness of states to characterise actions as a use of force when the consequences are apparent.[258] Traditionally, armed forces carried out operations that qualified as a use of force and their effects were measurable (such as battle damage assessments), while with cyberattacks, consequences may be less evident. Therefore, the more identifiable and quantifiable a set of consequences of a cyberattack are,

[251] Ibid at 50
[252] Ibid.
[253] Ibid.
[254] Ibid.
[255] Ibid.
[256] Ibid.
[257] Ibid.
[258] Ibid at 51.

the easier it will be to determine whether a state has reached the level of a use of force.[259]

(f) Military character: if there is a link between a cyberattack and a military operation, this would increase the likelihood of a characterisation of a use of force.[260] According to the experts, this is supported by the Charter which is particularly concerned with military actions.[261]

(g) State involvement: The extent to which a state is involved in a cyberattack ranges from conducting it itself through armed forces to those in which its involvement is peripheral.[262] The clearer the nexus is between a state and the cyberattacks, the more likely they are to be considered to be uses of force.

(h) Presumptive legality: Because international law is generally prohibitive in nature, acts which are not expressly forbidden are generally permitted if there is not an accepted customary law prohibition.[263] According to the experts, international law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure per se, therefore acts falling into these categories are presumably legal and are less likely to be considered to be uses of force by states.[264]

According to the Tallinn Manual, these factors are not exhaustive and one would also need to look at the circumstances in which a cyberattack takes place in order to determine whether it is a use of force.[265] Additionally, states may look to other factors such as the prevailing political environment, whether the cyberattack is a sign of future military force, the identity of the attacker, any records of cyberattacks by the attacker, and the nature of the target – such as critical infrastructure - in making a use of force assessment.[266] These factors support my submission that non-violent cyberattack or those that do not rise to the threshold of an armed attack are capable of contravening article 2(4) of the UN Charter.

---

[259] Ibid.
[260] Ibid.
[261] Ibid.
[262] Ibid.
[263] Ibid at 52.
[264] Ibid.
[265] Ibid.
[266] Ibid.

SECTION D: CRITICAL INFRASTRUCTURE

An attack directed against the so-called 'critical infrastructures' seems to be the most conceivable non-violent cyberattack, or cyberattack which does not rise to an armed attack. As stated in chapter two, the Stuxnet worm was specifically meant to target critical infrastructures and systems which controlled pipelines, electric plants, nuclear facilities and other large industrial installations. The protection of critical infrastructures has always been a key concern for states in their discussion on cybersecurity.[267] The most recent example of this articulation was in UNGA Resolution 73/266,[268] where the sixth preambular paragraph states the following:

> *Expressing concern* that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States, to the detriment of their security in both civil and military fields.

The advantage of this concept is that it is widely used by states and multilateral organisations in the discussion of cybersecurity and seems to address their key concerns.[269] Additionally, while there is some variation on the interpretation of the term, there is sufficient overlap and consistency to provide a general understanding of the meaning of the term. Below, I will discuss various definitions of 'critical infrastructures' which have been adopted by both states and international organizations in order to better understand the concept.

(a) UN General Assembly:

> Critical infrastructure include '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.'[270]

[267] Nils Melzer Op Cit note 71 at 14.
[268] Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 22 December 2018.
[269] Nils Melzer Op Cit note 71 at 14.
[270] Ibid

(b) United States:

> ‘Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both government and private.’[271]
>
> ‘The term ‘critical infrastructure’ means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.’[272]
>
> ‘The critical infrastructure sectors consist of agriculture and food, water, public health, emergency services, government, the defence industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and posting and shipping.’[273]

(c) Shanghai Cooperation Organisation:

> “‘Critical structures’ – public facilities, systems and institutions attacks on which may cause consequences directly affecting national security, including that of the individual, society and state.”[274]

(d) European Union:

> ‘Critical infrastructure include those physical resources, services, and information technology facilities, network and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.’[275]
>
> ‘Critical Information Infrastructure (CII): ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, internet, satellites, etc).’[276]

---

[271] Ibid at 15.
[272] Ibid.
[273] Ibid.
[274] Ibid.
[275] Ibid.
[276] Ibid.

(e) Australia:

> ‘Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic wellbeing of the nation or affect Australia’s ability to ensure national security.’[277]
>
> Critical infrastructures include: ‘banking and finance, communications, emergency services, energy, food chain, health (private), water service, mass gatherings, and transport (aviation, maritime surface).’[278]

This section identified critical infrastructures as the potential targets of cyberattacks which were either non-violent or fell below the threshold of an armed attack. In the UNGA Resolution above, states have already expressed their concern that cyberattacks could be aimed at their critical infrastructure. Therefore, this section tried to identify what ‘critical infrastructure’ entailed as states have been shown (both prior to the Second World War, to more recently, with the US’ retaliation on Iran which was curated to stay ‘well below the threshold of war’) to be eager to exploit legal ambiguities in order to attack states. Developing an understanding of critical infrastructures is therefore mandatory as an attack on them would form a crucial part in the victim state’s use of force assessment.

CONCLUSION

This chapter submitted the argument that ‘force’ in article 2(4) could be interpreted to prohibit the use of cyberattacks. I submit that ‘force’ was not intended to have a singular meaning. To support this argument, I attempted to show that the ultimate aim of the drafters was to prevent interstate conflict, and that the term ‘force’ originated due to the need to prevent states from exploiting linguistic loopholes, something that was prevalent before the Second World War. The drafters of the Charter excluded specific types of force, but this also implies that they left the door open for other types of force to fall within this provision. Had they wanted to limit the concept of force to armed force, they could have done so as the term is present in other parts of the Charter.

---

[277] Ibid.
[278] Ibid.

In addition to looking at the history surrounding the drafting of article 2(4), this section looked at various provisions in the UN Charter to support the argument that the use of cyberattacks contravenes this provision. After investigating the overall aims of the UN Charter, it would lead to 'manifestly absurd or unreasonable' conclusions if article 2(4) was interpreted narrowly to exclude the use of cyberattacks. Permitting cyberattacks would lead to cyberwar which could escalate to an armed conflict, contradicting the most important Purpose of the Charter, which is to maintain international peace and security.

The ICJ has alluded to the fact that generic terms are capable of evolving over time. A secondary - yet interlinked - argument that I have submitted is that 'force' is one such term that is capable of evolving over time. This chapter provided numerous examples of how the concept of force has changed since the UN Charter was first adopted to support this assertion.

Finally, this section discussed critical infrastructure and factors that states would consider when making use of force assessments for cyberattacks which fell below the threshold of an armed attack. I identified critical infrastructure as the likely targets of non-violent cyberattacks or those curated to fall below an armed attack.

It is important to correctly categorize cyberattacks as either being armed attacks, 'less grave' uses of force or as neither, because this will dictate what response the victim state is legally permitted to pursue. The following chapter will discuss the responses available to the victim state of a cyberattack. At the same time, in this chapter I will make the third of my overarching arguments, that existing international law is insufficient to adequately regulate the use of cyberattacks and that a multilateral treaty is required.

CHAPTER FIVE: INTERNATIONAL RESPONSES

This chapter has two aims: the first is to briefly discuss the current responses available to a state which is the victim of a cyberattack. The second is to argue that these responses are inadequate in dealing with the complex nature of cyberattacks, and that a multilateral treaty would be a better option to deal with cyberattacks.

This chapter will be divided as follows: Section A will briefly discuss the judicial and non-judicial responses that a victim state of a cyberattack may pursue. Due to international law's inability to create a response to cyberattacks as a use of force, this section will therefore investigate responses for traditional uses of force, and investigate whether these responses can be transposed to victim states of cyberattacks.

Section B will submit an argument for the adoption of a multilateral treaty. I submit that the existing international responses are inadequate in addressing the unique nature of cyberattacks and that a multilateral treaty would be a better alternative to maintain international peace and security. To support this argument, I will refer to various treaties to identify various issues that would be better resolved by adopting a multilateral treaty.

SECTION A: EXISTING INTERNATIONAL LAW

When a belligerent state commits an unlawful use of force, it commits an internationally wrongful act which entitles the victim state to respond in numerous ways. This section will investigate the judicial and non-judicial responses available to the victim state of a use of force and discuss whether these can be transposed to the victim state of a cyberattack.

(a) Judicial responses

The first response available to a victim state is to approach the ICJ to seek numerous remedies found in the International Law Commission's Draft Articles on State Responsibility (Draft Articles). States have turned to the ICJ to resolve alleged uses of force on a number of cases beginning with the *Corfu Channel*[279] case which was

[279] (United Kingdom of Great Britain and Northern Ireland v. Albania) (1949) ICJ.

decided in 1949, to most recently in the *Armed Activities on the Territory of the Congo*[280] case which was decided in 2005.

The remedies which the victim state of a use of force may invoke are found in articles 29-37 of the Draft Articles. These are: the continued duty of performance,[281] cessation and non-repetition,[282] and reparations[283] which take the form of restitution[284], compensation[285] and satisfaction.[286]

Based on the remedies in the Draft Articles, it appears that the remedies available for traditional uses of force can be transposed to the victim states of a cyberattack. This is because the victim state of a cyberattack would want the same remedies, such as the cessation and non-repetition of the cyberattacks along with reparations for the damage suffered.

However, I submit that the judicial option is inadequate for numerous reasons. The first relates to the amount of time that it takes to reach a ruling in the ICJ. I submit that the ICJ is not responsive enough to keep up with the rapid nature of cyberattacks. This is based on the significant amount of time between when the alleged use of force occurred and when the ICJ makes its final judgment. In the *Corfu Channel* case, the initial use of force occurred in 1946 and the ICJ issued its judgment in 1949. The ICJ ruled on the *Nicaragua case* in 1986, seven years after the alleged use of force. Finally, the *Democratic Republic of Congo v. Uganda* case was decided in 2005, seven years after the unlawful use of force.

A second reason that I submit that the judicial option is inadequate for the victim states of cyberattacks is because of the unique and rapid nature of cyberattacks. A devastating amount of damage can be done in one day using cyberattacks. In 2009, the United States claimed that it suffered over 50,000 cyberattacks per day.[287] Chapter two of this dissertation discussed the devastation that could be caused

---

[280] (Democratic Republic of Congo v. Uganda) (2005) ICJ.
[281] Article 29.
[282] Article 30.
[283] Article 31.
[284] Article 35.
[285] Article 36.
[286] Article 37.
[287] James Carden 'Time to pursue an international cyber treaty?' *The Nation* 30 April 2019 available at *https://www.thenation.com/article/international-cyber-treaty-russia-china-dnc/* accessed on 19 December 2019.

through the use of cyberattacks, and I submit that 50,000 cyberattacks with the intention to cause severe damage on one day could cause irreparable damage. I further submit that the damage suffered by the victim state would be multiplied exponentially if attacks continued until the ICJ ruled on the matter (or until provisional measures are granted). Additionally (and depending on the nature of the cyberattacks), I submit that the remedies in the Draft Articles are either not responsive enough to deal with cyberattacks (cessation and non-repetition for example is not responsive enough in the case of cyberattacks which are rapid, which effectively eliminates the need for this remedy as attacks may have ceased by the time legal proceedings are instituted) or will not adequately compensate the victim state for the damage it has suffered. I submit that a treaty would be proactive in trying to prevent cyberattacks as opposed to the judicial option which is reactive.

Thirdly, the ICJ in previous use of force cases has awarded compensation to the victim state of a use of force. However, the ICJ has ruled that it would decide on the quantum of compensation only *after* the parties have failed to reach a settlement on the compensation to be paid by the responsible state. An example of this is the *Democratic Republic of Congo v. Uganda* case where the ICJ ruled that the Uganda had violated the prohibition on the use of force and that the Democratic Republic of Congo was entitled to reparations.[288] But the ICJ would only decide on the quantum of the compensation should both parties not be able to reach a settlement on the amount.[289]

Furthermore, the ICJ has not always been able to enforce their judgments for compensation and the *Nicaragua* case is the most famous example of this. Here, the ICJ ruled that the US was to pay compensation amounting to $12 billion to Nicaragua.[290] However, after numerous unsuccessful attempts to enforce the

[288] Nigel D. White, Christian Henderson *Research handbook on international conflict and security law*: *Jus ad Bellum, Jus ad Bello and Jus Post Bellum* (2013) at 643.
[289] Ibid.
[290] Mary Ellen O'Connell 'The Prospects for Enforcing Monetary Judgments of the International Court of Justice: A Study of Nicaragua's Judgment Against the United States' (1990) *Maurer Faculty Paper* at 891.

judgment, Nicaragua eventually gave up on its attempts to obtain compensation from the US.[291]

(b) Non-judicial responses

The Draft Articles also contain the non-judicial responses that a victim state of a use of force may pursue. These responses can be found in articles 20-25 of the Draft Article and are: consent,[292] self defence,[293] countermeasures,[294] force majeure,[295] distress[296] and necessity.[297] As self defence was discussed in chapter three, the only response available to a use of force falling below the threshold of an armed attack is the use of countermeasures.

Countermeasures are invoked in circumstances where one state commits a wrongful act against another state and the victim state resorts to non-forcible countermeasures in order to procure its cessation and to achieve reparation for the injury sustained.[298] Essentially, they are the mechanism in which international law allows parties to carry out self help.[299] In the *Gabčíkovo-Nagymaros Project* case, the ICJ accepted that countermeasures might justify otherwise unlawful conduct which was taken in response to a previous internationally wrongful act of another state and directed against the state which committed the wrongful act.[300]

The commentary to the Draft Articles (in Chapter II Part Three) outlines numerous limitations (based on articles 49-53) in the use of countermeasures in order to safeguard against abuse.

---

[291] Lan Nguyen and Truong Minh Vu 'After the Arbitration: Does Non-Compliance Matter?' *Asia Maritime Transparency Initiative* (2016) available at *https://amti.csis.org/arbitration-non-compliance-matter/* accessed on 17 December 2019.
[292] Article 20.
[293] Article 21.
[294] Article 22.
[295] Article 23.
[296] Article 24.
[297] Article 25.
[298] International Law Commission 'Draft Articles on Responsibility of States Intentionally Wrongful Acts, With Commentaries' (2001) *Yearbook of the International Law Commission* at 75 para 1.
[299] Mary Ellen O'Connell and Louise Arimatsu 'Cyber Security and International Law' (2012) available at *https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf* at 8 accessed on 15 December 2019.
[300] International Law Commission Op Cit note 300 at 75 para 2.

These are:

1. They must be directed at the state which has committed the wrongful act and not a third state;[301]
2. They are to be non-forcible measures;[302]
3. Since countermeasures are intended to be instrumental – seeking the cessation of an international wrong and obtaining reparations for injury suffered – they are temporary in character and must be, as far as possible, reversible in their effects in terms of future legal obligations between the two states;[303]
4. They must be proportionate;[304]
5. They must not deviate from certain basic obligations, in particular peremptory norms;[305]
6. Countermeasures cannot affect any dispute settlement procedure which is in force between the two states and applicable to the dispute;[306]
7. Countermeasures may not be used to impair diplomatic and consular inviolability;[307]
8. Countermeasures must be preceded by a demand by the injured state that the responsible state comply with its obligations, and this demand must be accompanied with an offer to negotiate;[308] and
9. Countermeasures must be suspended if the internationally wrongful act has ceased and the dispute is submitted in good faith to a court or tribunal with the authority to make a binding decision on the parties.[309]

The Tallinn Manual also repeatedly supports my submission that states may rely on countermeasures when they are victims of cyberattacks falling below the threshold of an armed attack.[310] However, I submit that countermeasures are also inadequate for numerous reasons.

---

[301] Ibid at 129 para 6.
[302] Ibid.
[303] Ibid.
[304] Ibid.
[305] Ibid.
[306] Ibid para 7.
[307] Ibid.
[308] Ibid.
[309] Ibid.
[310] Michael N. Schmidt Op Cit note 80 at 26, 35, 41 and 52.

The first reason that countermeasures are inadequate is because they pose a particular danger when it comes to cyberattacks: that this could lay the groundwork for a cyberwar between states which could then escalate to a conventional war. In 2019, Forbes revealed that governments were becoming more 'cyber' and had built so-called 'red team's that carried out offensive cyberattacks ranging from espionage and propaganda, to assaults on infrastructure and stolen money or intellectual property.[311] This article also stated that governments were becoming more aggressive with their cyber campaigns and were breaking certain unspoken rules of engagement.[312] I submit that the use of cyberattacks as a countermeasures is likelier to escalate to a cyberwar (and potentially a traditional war) than it is to obtain compliance from the belligerent state.

States have already started contemplating using cyberattacks as countermeasures. The UK became the first state to announce that it was developing offensive cyber capabilities as part of its deterrent strategy.[313] In 2018, the UK considered launching a cyberattack as a countermeasure, but opted to exercise restraint until rules of engagement could be established.[314]

The second reason relates to the limitations discussed above in the Draft Articles. According to the Draft Articles, countermeasures are intended to bring about the cessation of wrongful conduct and must be suspended when the internationally wrongful conduct has ceased. This poses problems for the state which is either the victim of a singular attack, or composite attacks.

As countermeasures are intended to bring about the cessation of internationally wrongful conduct, it suggests that a victim state may not rely on countermeasures for singular or composite cyberattacks as these attacks could not be interpreted as being 'ongoing'. I submit that victim states are unlikely to tolerate cyberattacks without

---

[311] Corey Nachreiner 'Can we wait any longer for a Multinational cyber treaty' available at *https://www.forbes.com/sites/forbestechcouncil/2019/02/19/can-we-wait-any-longer-for-a-multinational-cyber-treaty/#50103bb52fb3* accessed on 5 January 2020.
[312] Ibid.
[313] World Economic Forum 'Can state cyber attacks be justified under international law' (2018) available at *https://www.weforum.org/agenda/2018/04/can-offensive-cyber-attacks-be-justified-under-international-law/* accessed on 18 December 2019.
[314] Ibid.

responding and may respond with their own cyberattacks, which may escalate to a cyberwar and potentially a conventional war.

Thirdly, evidence of the perpetrator of a cyberattack is often found when the damage is done and the act is over. This means that a victim state can only legally employ countermeasures against cyberattacks when the identity of the perpetrator is revealed and the attacks are still ongoing, along with the other requirements listed above. Again, this creates a situation where a victim state is forced to endure cyberattacks from another state and is not permitted to legally respond with countermeasures because certain conditions are no longer present. I submit that victim states are unlikely to tolerate these attacks without responding.

In conclusion, although the victim state of a cyberattack falling below the threshold of an armed attack may legally respond with countermeasures, I submit that countermeasures are also inadequate in dealing with cyberattacks. This is because there are numerous loopholes that can be exploited by the responsible state whereby that state can use a cyberattack against the victim state and the victim state may not legally respond with countermeasures. This creates a situation in which victim states are forced to endure cyberattacks and may not respond legally. I submit that victim states are unlikely to endure such attacks indefinitely but are likely to respond with cyberattacks and this could escalate to a cyberwar, which could then conceivably escalate to a conventional war.

SECTION B: MULTILATERAL TREATY

I submit that the creation of a multilateral treaty is the best option to maintain international peace and security. I submit that a treaty is better suited to maintain international peace and security than the current options in extant international law because it would proactively prevent the use of cyberattacks, it would eliminate many of the loopholes surrounding the use of cyberattacks and finally, a treaty can address numerous issues that have surrounded cyberattacks, some of which will be discussed below.

Additionally, states can no longer remain apathetic about a multilateral treaty as cybersecurity is a problem for the international community as a whole, not just interested states. An example of this collective vulnerability was evident in 2017 during the ‘WannaCry’ cyberattacks. This cyberattack affected over 200,000

computers in over 150 countries resulting in damages of over $4 billion, including shutting down the UK's health services.[315]

I submit that a multilateral treaty offers the best prospects of maintaining international peace and security, and it would be able to address numerous issues that exist surrounding cyberattacks. This section will therefore discuss numerous issues that currently exist in international law that would be addressed by a treaty. This section will predominantly draw on the most recent multilateral cybersecurity treaty, the EU Cybersecurity Act,[316] which came into effect on 27 June 2019, but will also draw on other treaties as well.

A multilateral treaty will offer specificity and clarity on the following critical issues surrounding cybersecurity:

(a) Norms

A multilateral treaty is unlikely to call for a complete ban on state activities on the internet as that would be impractical. Instead, such a treaty would likely be a 'dual-use' treaty such as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and the Chemical Weapons Convention (CWC). Both of these treaties seek to ban the use and even possession of chemical and nuclear weapons, while at the same time promoting the legitimate, non-military use of chemical and nuclear weapons.[317] Examples are the six critical norms introduced by the Global Commission on the Stability of Cyberspace (GCSC) in November 2018.[318] These are the norm to avoid tampering,[319] the norm against commandeering of ICT Devices into botnets,[320] the norm for states to create a vulnerability equities process,[321] the norm to reduce and mitigate significant vulnerabilities,[322] the norm on basic cyber hygiene as

[315] Corey Nachreiner Op Cit note 313.
[316] No 526/2013 (2019).
[317] Mary Ellen O'Connell and Louise Arimatsu Op Cit note 301 at 9.
[318] Global Commission on the Stability of Cyberspace 'Norm Package Singapore' Available at *https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf* accessed on 5 January 2019.
[319] Ibid at 8.
[320] Ibid at 10.
[321] Ibid at 12.
[322] Ibid at 14.

foundational defence,[323] and the norm against offensive cyber operations by non-state actors.[324]

(b) Defining critical terms

Arguably the most important consequence of a multilateral treaty would be reaching international consensus on the definition of critical terms. As has been shown in previous chapters, international law is still lacking consensus on critical terms such as 'force', 'weapon' and 'cyberweapon'. A treaty which defines critical terms in cybersecurity will ultimately be beneficial for international law and the UN's collective security regime.

(c) Which organisation is responsible to reach treaty objectives?

A multilateral treaty would outline which body is tasked with the implementation of the treaty to achieve its goals. This clarity is better than the fragmented nature that currently exists in international law. The EU Cybersecurity Act, for example, tasks ENISA (European Union Agency for Cybersecurity) with the aim of achieving the goals of the treaty.[325]

(d) Jurisdiction

A multilateral treaty would clarify which judicial body is to settle a dispute and what conditions need to be satisfied before that tribunal can be approached. The treaty could confer jurisdiction on an existing tribunal such as the ICJ, a new judicial body could be created which specifically deals with contraventions of the treaty such as the United Nations Compensation Commission (UNCC) for example,[326][327] or the treaty could allow disputes to be resolved by the Security Council. Examples of the latter are the CWC and NPT which empower the General Assembly and Security Council to intervene for grave and severe violations of the respective conventions.[328]

[323] Ibid at 16.
[324] Ibid at 18.
[325] Article 3(1).
[326] A subsidiary of the Security Council created by Security Council Resolution 678 (1991) to process claims for damage and losses suffered due to the Iraq's invasion of Kuwait.
[327] UNCC 'UNCC at a Glance' available at *https://uncc.ch/uncc-glance* accessed 16 December 2019.
[328] Mary Ellen O'Connell and Louise Arimatsu Op Cit note 301 at 9.

(e) Consequences for breaches

A multilateral treaty will provide clarity on what punishments will be imposed for a breach of the treaty. The treaty will not only clarify the consequences between the responsible state and victim state but would also clarify the consequences between the responsible state and other parties to the convention. An example of such consequences are collective sanctions.

(f) Measures to be taken at national level

As the aim of the treaty would be to promote collective security, the Treaty could specify what measures states can take at the domestic level to aid in the pursuit of the goals of the treaty. These measures could include but are not limited to: the creation of domestic laws; creating or supporting enforcement agencies; and, partnerships with non-state actors to aid in the pursuit of the goals of the treaty.

(g) Exchanging knowledge, know-how and best practices

Just like the EU Cybersecurity Act,[329] the proposed treaty could promote the sharing of knowledge and practices between states as they seek to maintain peace and security in cyberspace. The exchange of information and practices will assist less developed states to develop their capacity in order to meet the objectives of the treaty.

(h) Cooperation models on how to address trans-border issues

'WannaCry' showed the trans-border nature of cyberattacks. A treaty will bring states together to find ways to co-operate in order to address these issues.

CONCLUSION

Although international law currently offers recourse for victims of cyberattacks, I submit that it is not sufficient to avoid cyberwar, which could possibly escalate to traditional war. This is because existing international law is either not reactive enough and cannot prevent attacks, it is not responsive enough after one cyberattack to prevent a response from the victim state, and there are currently no deterrents strong enough to prevent states from using cyberattacks.

[329] Article 7(2)(a).

In this chapter, I also discussed countermeasures which are the only legal non-judicial response available for a use of force which falls below the threshold of an armed attack. However, the limitations placed on the victim state which seeks to use countermeasures means that a belligerent state can exploit loopholes to create conditions where it can attack the victim state and that state may not legally be permitted to respond with countermeasures. This means that the victim state is essentially forced to tolerate attacks against it by the belligerent state. I submit that this threatens international peace and security because states are unlikely to tolerate these attacks indefinitely and may respond with their own cyberattacks which may escalate to cyberwar, which may possibly escalate to a conventional war.

A multilateral treaty offers the best prospects of maintaining international peace and security because it would proactively attempt to prevent the use of cyberattacks. This approach would differ from existing responses which are reactive. A treaty offers numerous advantages that will lead to the maintenance of international peace and security such as defining critical terms, establishing cybersecurity norms which could become customary, and encouraging co-operation between states in dealing with certain trans-boundary issues. As ‘WannaCry’ showed, cybersecurity is a concern for the entire international community and states can no longer remain indifferent to cybersecurity concerns.

CHAPTER SIX: CONCLUSION

This dissertation set out to make three interrelated arguments. The first was that cyberweapons were weapons, the second was that cyberattacks were a use of force, and finally, that the adoption of a multilateral treaty offered the best prospects of maintaining international peace and security.

Establishing that cyberweapons were weapons was necessary for various reasons. The first is that it lay the foundation for my second argument as it is generally accepted that a state which unjustifiably attacks another state with other types of weapons commits an unlawful use of force. I wanted to show that it would be absurd for the prohibition to prohibit states from attacking each other with one type of weapon, but exclude states attacking each other with another type of weapon which is capable of causing similar damage. The second is that the use of cyberattacks is no longer limited to hacking and stealing sensitive information. Cyberattacks are now capable of producing devastating physical damage. When describing the potential damage that cyberattacks can cause, former FBI Director Robert Muller said that cyberattacks could have the same effect as a well placed bomb. The final, and perhaps the most important reason it was important to establish that cyberweapons are weapons is because states are in fact using them as weapons. In the second chapter I provided numerous examples of states using cyberweapons alongside, or as an alternative to traditional weapons to show that states have in fact begun to militarize cyberspace.

The militarization of cyberspace provided a perfect segue to my second argument, which was that cyberattacks were a use of force. Supporting this assertion provided me with numerous difficulties, the most obvious being that there was no internationally accepted definition for what ‘force’ was, both in and out of cyberspace. However, there is consensus among some commentators that ‘force’ in article 2(4) of the UN Charter initially referred to armed or military force. The second challenge that was faced was whether only the ‘violent’ cyberattacks constituted a use of force or whether non-violent cyberattacks could also constitute a use of force. I believed that both violent and non-violent cyberattacks were capable of contravening article 2(4) of the UN Charter.

Chapters three and four of this dissertation were split along the same lines that the ICJ in the *Nicaragua* case divided the concept of force. Chapter three argued that cyberattacks were an armed attack or 'most grave' use of force, while chapter four argued that cyberattacks could also be a 'less grave' use of force. I chose to separate the two for multiple reasons. The first is that it is important to determine which category a cyberattack falls into as this will determine the response the victim state is able to pursue legally. The second is to shed light on what non-violent cyberattacks and cyberattacks which do not rise to the threshold of an armed attack would look like.

Chapter three argued that cyberattacks could be an armed attack. This submission was supported by the Tallinn Manual where international law experts agreed that cyberattacks could be an armed attack if the *scale and effects* of the cyberattack reach the threshold of an armed attack.

Chapter four might initially seem unnecessary because if cyberattacks can be a 'most grave' use of force then they automatically can be a 'less grave' use of force. I submit that this investigation was necessary because states are already curating their attacks to fall below the threshold of an armed attack in order to exploit the ambiguity which surrounds article 2(4) of the Charter. In order to successfully argue that the prohibition in article 2(4) extended to cyberattacks, it was important to establish what behaviour the drafters of the UN Charter were aiming to prohibit when the provision was drafted and adopted.

I relied on article 31 and 32 of the Vienna Convention on the Law of Treaties which requires you to look at the circumstances and context in which a treaty was drafted in order to confirm the meaning of a provision. An investigation into the context in which the provision was drafted reveals that article 2(4) was the culmination of numerous unsuccessful attempts by states to prevent interstate conflict. When referring to the *travaux preparatoires* of the UN Charter, they reveal that 'force' was used to avoid states exploiting loopholes in order to engage in conflict. The *travaux preparatoires* also reveal that certain types of force were excluded from the conception of 'force' in article 2(4) of the Charter, implying that other types of force were capable of falling within this prohibition. This supports my submission that the term should not be interpreted narrowly to mean military force but may include other

types of force. Had the drafters intended the prohibition to be limited to armed force, they could have simply used the term as it is present in other parts of the UN Charter. Other provisions within the Charter support the interpretation that the UN Charter is primarily concerned with avoiding war and maintaining international peace and security. I submit that an interpretation where the use of cyberattacks is excluded from the prohibition in article 2(4) would lead to a result which is manifestly absurd or unreasonable.

The Tallinn Manual also supports the submission that cyberattacks can be 'less grave' uses of force. Although much would depend on the circumstances of the particular attack, it does support the notion that cyberattacks *can* be 'less grave' uses of force. The Tallinn Manual goes on to provide a list of non-exhaustive factors that victim states could consider when making their use of force assessments.

Finally, chapter five made the argument that existing international law is unable to adequately regulate cyberattacks and that a multilateral treaty is required as it would be better equipped to maintain international peace and security. To support this argument, I discussed how international law is reactive, not responsive enough, and how a belligerent state could exploit loopholes in order to attack states without that state being able to legally respond. I submit that victim states are unlikely to endure those cyberattacks indefinitely and could respond with their own cyberattacks, which may then escalate to a cyberwar and then a traditional war. I submit that a multilateral treaty offers the best prospects of maintaining international peace and security as it would proactively attempt to prevent the use of cyberattacks and also provide clarity on many of the ambiguities surrounding cyberattacks.

BIBLIOGRAPHY

Primary Sources

Cases

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (2007) ICJ.

Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda) (2005) ICJ.

Certain Expenses of the United Nations: Advisory Opinion (1962) ICJ.

Corfu channel (United Kingdom of Great Britain and Northern Ireland v. Albania) (1949) ICJ.

Dispute Concerning Navigational and Related Rights (Costa Rica v. Nicaragua) (2009) ICJ.

Factory at Chorzów (Germany v. Poland) (1928) PCIJ.

Gabčíkovo-Nagymaros Project (Hungary v Slovakia) (1997) ICJ.

Legality of the Threat or the Use of Nuclear Weapons: Advisory Opinion (1996) ICJ.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States) (1986) ICJ.

Oil Platforms (Islamic Republic of Iran v. United States of America) (2003) ICJ.

Pulp Mills on the River Uruguay (Uruguay v. Argentina) (2010) ICJ.

The Caroline v. The United States, 11 U.S. (7 Cranch) (1813).

Treaties

Charter of the United Nations, 1945.

Chemical Weapons Convention, 1992.

Covenant of the League of Nations, 1919.

Regulation (EU) 2019/EU Cybersecurity Act, 2019.

Kellogg-Briand Pact, 1928.

The Locarno Pact, 1925.

Treaty on the Non-Proliferation of Nuclear Weapons, 1968.

Vienna Convention on the Law of Treaties, 1969.

Miscellaneous

Draft Article on Responsibility of States for Internationally Wrongful Acts, with Commentaries, 2001.

Draft Article on Responsibility of States for Internationally Wrongful Acts, 2001.

Statutes

Trading with the Enemy Act 1914 (United Kingdom).

Trading with the Enemy Act 1939 (United Kingdom).

United Nations General Assembly Resolutions

Resolution 1514 (XV): Declaration on the Granting of Independence to Colonial Countries and Peoples, 1960.

Resolution 2652 (XXV): Declaration on Principles of International Law concerning Friendly Relations and Cooperation among states in accordance with the Charter of the United Nations, 1970.

Resolution 73/266: Advancing responsible State behaviour in cyberspace in the context of international security, 2018.

United Nations Security Council Resolutions

Resolution 611: Israel-Tunisia, 1988.

Secondary Sources

Books

Bruno Simma, Daniel Erasmus-Khan, George Nolte, Andreas Paulus *The Charter of the United Nations: A Commentary* 3 ed (2012) Oxford University Press, Oxford, United Kingdom.

Frauke Lachenmann and Rudiger Wolfrum *The law of armed conflict and the use of force: the Max Planck Encyclopaedia of Public International Law* (2017) Oxford University Press, Oxford, United Kingdom.

Georg Kerschischnig *Cyberthreats and international law* (2012) Eleven International Publishing, The Hague, Netherlands.

Jens David Ohlin, Kevin Govern, and Claire Finkelstein *Cyberwar: Law and Ethics for Virtual Conflicts* (2015) Oxford University Press, Oxford, United Kingdom.

Marc Weller *The Oxford Handbook of the Use of Force in International Law* (2015) Oxford University Press, Oxford, United Kingdom.

Michael N. Schmidt *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) Cambridge University Press, Cambridge, United Kingdom.

Nigel D. White *Advanced introduction to international conflict and security law* (2014) Edward Elgar Publishing, Cheltenham, United Kingdom.

Nigel D. White, Christian Henderson *Research handbook on international conflict and security law: Jus Ad Bellum, Jus ad Bello and Jus Post Bellum* (2013), Edward Elgar Publishing Limited, Cheltenham, United Kingdom.

TW Bennet and J Strug *Introduction to International Law* (2013) Juta, Claremont, Cape Town.

William H. Boothby *Weapons and the law of armed conflict* 2ed (2016), Oxford University Press, Oxford, United Kingdom.

Journal Articles

Claire Oakes Finkelstein and Kevin H. Govern 'Introduction: Cyber and the Changing Face of War' (2015) *Faculty Scholarship Paper* 1566.

Cordula Droege 'Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) *International Review of the Red Cross.*

Jonathan A. Ophardt 'Cyber Warfare and the Crime Of Aggression: The Need For Individual Accountability On Tomorrow's Battlefield' (2010) *Duke Law & Technological Review no 3.*

Louise Arimatsu ‘A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations’ (2012) *NATO CCD COE Publications.*

Mary Ellen O’Connell ‘The Prospects for Enforcing Monetary Judgments of the International Court of Justice: A Study of Nicaragua’s Judgment against the United States’ (1990) *Maurer Faculty Paper*.

Matthew C. Waxman ‘Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)’ (2011) *Yale Journal of International Law*.

Nils Melzer ‘Cyberwarfare and International Law’ (2011) *The United Nations Institute for Disarmament Research*.

Oliver Kessler and Wouter G. Werner ‘Expertise, Uncertainty, and International Law’ (2013) *Leiden Journal of International Law*.

Thomas Rid & Peter McBurney ‘Cyber-Weapons’ (2012) *The Risi Journal*.

Internet References

Alex Kimani, ‘Why is Russia turning off its internet?’ *Safehaven Preservation of Capital* available at *https://safehaven.com/news/Breaking-News/Why-Is-Russia-Turning-Off-Its-Internet.html* accessed on 16 May 2019.

Corey Nachreiner ‘Can we wait any longer for a Multinational cyber treaty’ available at *https://www.forbes.com/sites/forbestechcouncil/2019/02/19/can-we-wait-any-longer-for-a-multinational-cyber-treaty/#50103bb52fb3* accessed on 5 January 2020.

Council on Foreign Relations ‘Cyberterrorism Hype v. Fact’ available at *https://www.cfr.org/expert-brief/cyberterrorism-hype-v-fact* accessed on 12 August 2019.

David E. Hoffman ‘Reagan Approved Plan to Sabotage Soviets’ *The Washington Post* 27 February 2004, available at *https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/?noredirect=on* accessed on 12 August 2019.

Global Commission on the Stability of Cyberspace 'Norm Package Singapore' Available at *https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf* accessed on 5 January 2019.

Harry Pettit 'CYBER WARS Russia set to test turning internet OFF to defend against US cyberattack' *The Sun* available at *https://www.thesun.co.uk/tech/8401797/russia-vs-us-cyber-war-games/* accessed on 16 May 2019.

James Carden 'Time to pursue an international cyber treaty?' *The Nation* 30 April 2019 available at *https://www.thenation.com/article/international-cyber-treaty-russia-china-dnc/* accessed on 19 December 2019.

Lan Nguyen and Truong Minh Vu 'After the Arbitration: Does Non-Compliance Matter?' *Asia Maritime Transparency Initiative* (2016) available at *https://amti.csis.org/arbitration-non-compliance-matter/* accessed on 17 December 2019.

Marc Schack 'Did the US stay "well below the threshold of war" with its June cyberattack on Iran?' available at *https://www.ejiltalk.org/did-the-us-stay-well-below-the-threshold-of-war-with-its-june-cyberattack-on-iran/* accessed on 7 October 2019.

Mary Ellen O'Connell and Louise Arimatsu 'Cyber Security and International Law' (2012) available at *https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf* at 8 accessed on 15 December 2019.

Nam Khoa Nguyen 'The international humanitarian law implications of the Tallinn Manual' available at *https://www.e-ir.info/2014/02/12/the-international-humanitarian-law-implications-of-the-tallinn-manual/* accessed on 7 November 2019.

National Cyber Security Centre 'Reckless campaign of cyber attacks by Russian military intelligence service exposed' available at https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed accessed 7 October 2019.

Norton ‘Zero-day Vulnerability: What is it, and How it Works’ available at *https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html* accessed 3 August 2019.

Phil Stewart ‘Analysis: Could a cyber war turn into a real one for the U.S.?’ available at *https://www.reuters.com/article/us-usa-cyber-pentagon/analysis-could-a-cyber-war-turn-into-a-real-one-for-u-s-idUSTRE74U75420110531* accessed on 9 November 2019.

Politico ’Weapons of Mass Disruption’ (2009) available at *https://www.politico.com/story/2009/05/weapons-of-mass-disruption-023099* accessed 12 August 2019.

Reuters ‘FBI Director Robert Mueller warns of growing cyber threat, could affect gov’t, business, individuals’ 5 March 2010 *NY Daily news* available at *https://www.nydailynews.com/news/money/fbi-director-robert-mueller-warns-growing-cyber-threat-affect-gov-business-individuals-article-1.174257* accessed on 16 May 2019.

Risi ‘CIA Trojan Causes Siberian Gas Pipeline Explosion’ available at *https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion* accessed 2 august 2019.

RT ‘FBI: Cyber Attacks – America’s Top Terror Threat’ 2 March 2012 available at *https://www.rt.com/news/cyber-fbi-security-mueller-691/* accessed on 31 March 2019

UNCC ‘UNCC at a Glance’ available at *https://uncc.ch/uncc-glance* accessed 16 December 2019.

United States Department of Defence ‘DOD Dictionary of Military Terms’ (2018) available at *https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf* accessed 12 August 2019.

UNSCR ‘Resolution 611’ available at *http://unscr.com/en/resolutions/611* accessed 7 October 2019.

World Economic Forum ‘Can state cyber attacks be justified under international law’ (2018) available at *https://www.weforum.org/agenda/2018/04/can-offensive-cyber-attacks-be-justified-under-international-law/* accessed on 18 December 2019.