HADEEL SALMAN

EXAMINING PROPORTIONATE RESPONSES TO STATE-SPONSORED CYBER-OPERATIONS

LAWS 592: LLM RESEARCH PAPER
SUPERVISOR: PROFESSOR ALBERTO COSTI

FACULTY OF LAW

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

2021

Abstract

In recent years there has been a rise in state-sponsored cyberattacks. There is a continuing debate among scholars, states and international institutions on how the UN Charter can apply to cyber-operations. My dissertation seeks to understand how the UN Charter can apply and what are the appropriate responses open to victim states that have been subject to a cyberattack. More specifically, the dissertation will outline the conditions required to satisfy a state's right to self-defence in cyberspace and note the limitations of responding to a state-sponsored cyberattack. It will highlight possible reforms and standards required to address the emerging threat of cyberspace. The dissertation is particularly concerned with cyberspace in the context of jus ad bellum. It will not discuss the notion of cyberwar or the principles of jus ad bello.

Word length

The text of this paper (including abstract, table of contents, footnotes and bibliography) comprises 34,999 words.

Subjects and Topics

Cyberspace – United Nations Charter – Use of Force – Self-defence – Attribution

Acknowledgements

I dedicate this dissertation to my baba and mama. Your love and sacrifice has guided me through it all.

I want to thank my dear sister Sara and my brother-in-law Daniel. Thank you for always being there. Thank you for letting me ramble and hash out my ideas with you.

Thank you to Rawa'a for encouraging me to pursue my Masters. Thank you to my oldest brother, Abdulla, who would send me little surprise gifts to get me through the difficult times. My littlest, Ahmed, for calling me on my late walks from the library to make sure I got home safely. And my cutest little niece, Ella, your artwork and poems fill my room with colour and joy.

My dearest friends and flatmates who have reminded me to celebrate the progress and success of my Masters. Thank you.

Thank you to Dr Marcin Betkier for sitting down with me to discuss some of the technical aspects of cyberspace. While I couldn't incorporate all aspects of our discussion into my dissertation, I am grateful to have been able to gain valuable knowledge concerning the field of cyberspace.

Finally, I want express my sincerest gratitude to my supervisor, Professor Alberto Costi. Thank you for dedicating your time and effort to guide me through this dissertation. You reassured me when I had doubts about my own capabilities and arguments. You have helped advance my understanding and passion for international law in cyberspace and I am proud of my dissertation. Thank you.

Contents

I Introduction

The world has become increasingly dependent on computer networks and digital infrastructures. As we grow increasingly reliant on digital technology, our digital infrastructure become more vulnerable to cyberattacks. Indeed, cyberspace provides a new platform for states to exercise their social, political and economic powers. As a result, the 2015 United Nations Group of Governmental Experts on *Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGGE) made it abundantly clear that the United Nations Charter "applies in its entirety".[1] However, cyberspace has novel and complex implications for international law. My dissertation will examine the challenges of applying the existing principles of *jus ad bellum* to the field of cyberspace and evaluate how states may respond to a cyberattack.

Part I will define the scope of cyberspace and explain that the field of cyberspace does not neatly fit within traditional domains. It will look at different definitions of what can constitute a "cyber-weapon". The Chapter will end by noting that not all cyber-conduct will meet the definition of a cyberattack. My dissertation is explicitly concerned with cyberattacks in the context of inter-state relations.

Part III begins by explaining how Article 2(4) UN Charter fails to address the effects of most cyber-operations that have occurred to date. It will demonstrate the shortfalls of Article 2(4) by evaluating the effects of the Stuxnet cyberattack and the 2016 United States electoral hacking. The Chapter will argue that Article 2(4) is not subject to a *de minimis* threshold of violence.[2] This is important to note because states that have undergone an offensive cyber-operation that falls below the threshold of force, will be legally limited in their responses.

Part IV will examine a new approach to cyber-force. It will scrutinise the principle of non-intervention and how it may be re-examined to include state-sponsored cyber-disinformation campaigns.

---

1 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* GA Res 70/174, A/Res/70/174 (2015) at 12.

2 Tom Ruys "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?" (2014) AJIL 159 at 159.

Part V will address state-on-state cyber-activities and discuss the challenges of attribution in cyberspace.[3] This area of cyberspace is especially complex because computers are easily accessible and can be weaponised by the general public. It will therefore determine that a high threshold of attribution must be established in cyberspace. It will argue that circumstantial evidence will be a sufficient standard of evidence to demonstrate responsibility in cyberspace.[4]

Part VI will discuss the doctrine of self-defence and examine how the elements of necessity, immediacy and proportionality may be applied in cyberspace. It will discuss the recent cyber-conflict between Iran and Israel to help demonstrate the difficulties of applying the orthodox principles of self-defence in cyberspace. It will end by briefly outlining the doctrine of collective self-defence and note the benefit of its application.

Part VII will critically review international documents, national statements and existing state practice to help determine the appropriate responses open to victim states in cyberspace.

Finally, Part VIII will discuss guidelines that may help alleviate the international risks of cyber-conflict. It will look at whether a regional cyber-treaty may help establish an appropriate framework for international cyber-norms. Part VI will end by debating whether the international community may benefit from an independent agency to help establish attribution in cyberspace.

II Fifth Domain

This part will define cyberspace and identify the most common cyber-weapons used to conduct state-sponsored cyberattacks. An examination of the terminology will be relevant when assessing the challenges of applying the UN Charter in cyberspace.[5]

A Cyberspace

3 James Lewis "Fighting the Wrong Enemy, aka the Stalemate in Cybersecurity" (26 November 2017) The Cipher Brief <www.thecipherbrief.com>.

4 Sharngan Aravindakshan "Cyberattacks: a look at evidentiary threshold in International Law" (2020) IJIL 286 at 286.

5 Erica Borghard and Jacquelyn Schneider "Russia's Hack Wasn't Cyberwar. That Complicates US Strategy" (17 December 2020) Wired < www.wired.com>.

Cyberspace is a new human-made domain that defies natural and geopolitical borders.[6] It has become increasingly weaponised in recent years as states have built offensive cyber-capabilities that are capable of targeting and destroying critical infrastructure or temporarily debilitating computer networks.[7] States view cyberspace as a new strategic location that can be used to advance their national objectives.[8] While cyberspace is a-territorial and does not share the physical characteristics of other domains, including air, land and sea, it is not exempt from international regulation.[9] However, the international legal framework has not provided a comprehensive definition of "cyberspace".[10]

More importantly, states have yet to reach consensus regarding its definition. In 2019, New Zealand's Cyber Security Strategy defined "cyberspace" as "the global network of interdependent information systems, telecommunications networks and information technology infrastructures".[11] Qatar extended its definition of "cyberspace" to include its users, adding that cyberspace is:[12]

> A virtual or electronic environment that results from the interdependent network of information and communications technology (e.g., the Internet, telecommunications networks, computer systems, and embedded processors and controllers) that links people with services and information.

The Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual"), a highly influential study sponsored by NATO, emphasises the operation of data and defines "cyberspace" as "the environment formed by physical and non-physical components, characterized using computer and electro-magnetic spectrum, to store, modify and exchange

---

6 Nicholas Tsagourias "The Legal Status of Cyberspace" in Nicholas Tsagourias and Russell Buchan (eds) *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, Cheltenham, 2015) 13 at 15.

7 Mette Eilstrup-Sangiovanni "Why the World Needs an International Cyberwar Convention" (2017) PT 380 at 382.

8 At 382.

9 Tsagourias, above n 6, at 13.

10 At 13.

11 Department of the Prime Minister and Cabinet "New Zealand's Cyber Security Strategy 2019" (July 2019) DPMC <https://dpmc.govt.nz> at 16.

12 Ministry of Information and Communications Technology "Qatar National Cyber Security Strategy" (May 2014) MOTC <https://www.motc.gov.qa> at 23.

data using computer networks".[13] Kenya, Finland and the United Kingdom share a similar definition and note the importance of protecting data infrastructures and networks.[14]

Defining the scope of "cyberspace" remains challenging. States have generally defined cyberspace in a manner that serves their strategic objectives and interests. Despite states providing different variations of "cyberspace", one component remains unchanged; all definitions acknowledge that "cyberspace" is an interconnected communication network.[15] Thus, for the purposes of my dissertation, I note Daniel Kuehl's definition of cyberspace:[16]

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies.

Prominent cyber scholar Nicholas Tsagourias adds to this definition and explains that there are three tiers that help make up the cyber-domain.[17] The first tier is made up of the physical infrastructures of cyberspace, namely, computers, wires and microprocessors.[18] The second tier is concerned with the operating systems and software of cyberspace.[19] Finally, the third tier is an extension of cyberspace and includes Internet Protocols and data packets.[20] Fundamentally, the physical aspects of cyberspace connect us to the virtual world of cyberspace.[21]

B Cyber-weapons

---

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

14 Binxing Fang *Cyberspace Sovereignty: Reflections on Building a Community of Common future in Cyberspace* (Springer, Singapore, 2018) at 23-24.

15 Tsagourias, above n 6, at 16.

16 Daniel Kuehl "From Cyberspace to Cyberpower: Defining the Problem" Franklin D. Kramer and others (ed) Cyberpower and National Security (University of Nebraska Press, Washington D.C, 2009) at 28.

17 Tsagourias, above n 6, at 15.

18 At 15.

19 At 15.

20 At 15.

21 At 15.

There is no internationally agreed definition of what constitutes a "cyber-weapon".[22] Weapons can come in different forms and should not be defined by their kinetic effects.[23] For example, there are international norms against the use of chemical and biological weapons because of their potentially lethal effects.[24] Despite having a non-kinetic effect, chemical agents can be considered as "weapons" in international law.[25] Thus, if an adversary uses a cyber-tool to exert offensive consequences, including psychological harm, destruction, or physical injury, that cyber-tool will be classified as a weapon, regardless of its non-kinetic effects.[26]

Rule 41 of the Tallinn Manual defines "cyber-weapon" as:[27]

> Cyber means of warfare that are by design, use or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack.

Accordingly, a cyber-weapon is a tool that is used to inflict harm, injury, violence or physical damage. The Manual notes that "injury" includes "serious and severe mental suffering".[28]

Nonetheless, the Tallinn Manual's definition is narrow because it strictly limits "cyber-weapons" to physical and psychological consequences.[29] The definition does not include cyber-activity that can affect the functionality of computer systems. It fails to acknowledge that cyber-weapons are different from other traditional weapons. Missiles and bombs, by their design, are intended to have injurious physical effects, whereas computers, by their design, are programmed to carry out day-to-day tasks. While computers can be weaponised to produce catastrophic kinetic effects, they are unlikely to be used in this way during peacetime.[30]

---

22 William H Boothby "Cyber weapons: oxymoron or a real world phenomenon to be regulated?" in Karsten Friis and Jens Ringsmose (ed) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (Routledge, London, 2016) at 165.

23 William H Boothby "Methods and Means of Cyber Warfare" (2013) 89 ILS 387 at 388.

24 At 389.

25 At 396.

26 Boothby, above n 22, at 166.

27 Tallinn Manual, above n 13, at 141.

28 Marco Roscini *Cyber Operations and the Use of Force in International Law* (Oxford University Press, Oxford, 2014) at 168.

29 At 168.

30 Boothby, above n 23, at 389.

Thomas Rid explains that a "weapon" is an "instrument of harm" and clarifies that a "cyber-weapon", includes "a computer code that is used, or designed to be used with the aim of threatening or causing physical, functional, or mental harm to structures, systems or living things".[31] For Rid, separating the concept of cyber-weapons from those that do not result in direct physical damage fails to encapsulate the different characteristics of malicious cyber-activity. In my opinion, Rid's definition is more accurate than the definition outlined by the Tallinn Manual because it encompasses the different effects of cyber-weapons.

C Cyberattacks

The Tallinn Manual narrowly defines "cyberattack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[32] It must interfere with a computer infrastructure and result in physical damage, death or injury.[33] The experts added that "interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components".[34] Thus, a cyberattack that compromises and disrupts the functionality of a computer network, will not fall within the definition, unless it results in physical destruction.

The consequential effect proposed by the Manual fails to address the most common effects posed by cyber-operations. During times of peace, cyber-operations are launched to impair the functions of a computer network without causing substantial physical damage. For example, in 2007, Russia allegedly launched a series of Distributed Denial of Service (DDoS) cyberattacks against Estonia.[35] This caused widespread disruption as Estonian citizens could not access essential sectors, including governmental websites and banking services.[36] Under the Manual's definition, the DDoS operations did not qualify as a 'cyberattack' because they did not result in damage, death or physical injury.

---

31 Thomas Rid *Cyber War Will Not Take Place* (C. Hurst Publishers Limited, Hurst, 2013) at 37.

32 Tallinn Manual, above n 13, at 106.

33 At 106.

34 At 108.

35 Emily Tamkin "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" (27 April 2019) Foreign Policy <https://foreignpolicy.com>.

36 Tamkin, above n 35.

I reject the approach taken by the Manual and instead adopt the definition developed by Hathaway, et al.[37] They explain that a cyberattack can include offensive and defensive action taken by a state or a non-state actor.[38] They note, "a cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose"[39] Firstly, the authors do not differentiate between the cyber-methods used to conduct the cyberattack, observing that an attack can "consist of any action" including hacking, infecting and infiltrating computer servers.[40] Secondly, they provide an objective assessment and argue that an attack must "undermine the functions" of a cyber-system to qualify as a "cyberattack".[41] It must destabilise or interfere with the functioning of cyber-systems.[42] Finally, the definition expressly states that a cyberattack must be launched for a "political or national security purpose".[43] The authors limit their definition to public international law and cyberattacks carried out by state actors and non-state actors. The definition acknowledges that cyberattacks are distinct from cybercrime or illicit cyber-behaviour, which are subject to different rules, procedures and responses.[44]

Furthermore, cyberattacks are different from cyber-espionage operations. Cyber-espionage does not directly impact the functions of computer servers and networks.[45] A cyberattack "must do more than passively observe a computer network or copy data".[46] For instance, in December 2020, Russia allegedly embedded a malicious software inside United States governmental systems.[47] The operation allegedly allowed Russian officers to gain access to computer networks and secretly gather sensitive and confidential information.[48] The hack does not fall within the definition of a "cyberattack" because it did not degrade the intended functions of

37 Oona A Hathaway and others "The Law of Cyber-Attack" (2012) 100 CLR 817 at 826.

38 At 826.

39 At 826.

40 At 826.

41 At 828. See also Reese Nguyen "Navigating "Jus Ad Bellum" in the Age of Cyber Warfare" (2013) 101 CLR 1079 at 1089; and General James E Cartwright "Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates: Joint Terminology for Cyberspace Operations" (November 2011) Homeland Security Digital Library <www.hsdl.org>.

42 At 826.

43 At 830.

44 At 831.

45 At 830. See also James Van de Velde "Cyber espionage is not cyber attack" (21 February) CYISRNET <www.defensenews.com>.

46 At 830.

47 Colin Dwyer "Pompeo Says Russia 'Pretty Clearly' Behind Cyberattack, Prompting Pushback From Trump" (19 December 2020) NPR <www.npr.org> at 1.

48 At 1.

United States computer networks.[49] The spyware must impair or destroy the computers system to fall within the scope of "cyberattack".

Economic cyber-espionage operations are treated uniquely. In 2010, China was accused of hacking into a number of corporate computer systems to steal trade secrets and intellectual property.[50] This was to advance their domestic interests and gain an economic advantage over the United States.[51] President Barak Obama condemned China's actions and in 2015, signed the United States-China Cyber Agreement to end economic cyber-espionage operations in their respective countries.[52]

I note this distinction because cyber-espionage operations are different from cyberattacks and raise different legal consequences. Indeed, states do not attempt to regulate political cyber-espionage operations in the same way as other malicious cyberattacks.[53] Cyber-espionage forms part of a state's cyber-defence strategy.[54] States aim to deter such operations by strengthening their own cyber-infrastructures, formally indicting hackers and launching their own counterintelligence operations.[55]

D Common Types of Cyberattacks

There are many different types of cyberattacks but for the purposes of my dissertation, I will focus on DDoS and malware. These are the most prevalent cyberattacks launched by states. They can disrupt online networks and systems, causing chaos, or they can target critical infrastructure and cause serious physical harm.

1 Distributed Denial of Service

49 Hathaway and others, above n 37, at 830. See also Borghard and Schneider, above n 5.

50 Sam Frizell "Here's What Chinese Hackers Actually Stole From U.S. Companies" (20 May 2014) Times <https://time.com>.

51 Frizell, above n 53.

52 U.S.–China Cyber Agreement United States-China (signed 25 September 2015) entered into force 25 September 2015.

53 Hathaway and others, above n 37, at 829. See also Glenn Sulmasy and John Yoo "Counterintuitive: Intelligence Operations and International Law" (2007) 28 MJ Intl Law 625 at 628.

54 At 829.

55 At 829.

DDoS attacks are the most common cyber-operations conducted by state actors.[56] DDoS cyberattacks infiltrate computer systems and release a flood of data that eventually overwhelms the network servers, rendering them ineffective.[57] Bot networks are launched using "zombie" computers. These "zombie" computers are "hijacked" to conduct and carry out malicious cyber-actions.[58] Essentially, the attack aims to deny a person or a group of people access to a network by overwhelming the network's data bandwidth and processing power.[59]

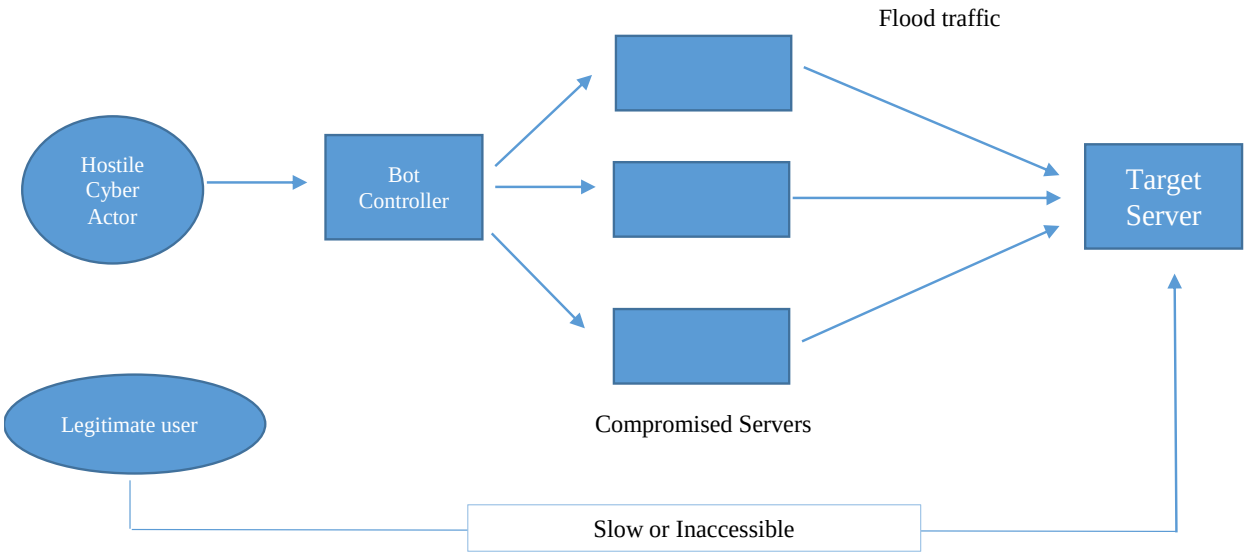

Figure 1 Architecture of DDoS Cyberattack [60]

DDoS cyberattacks are especially difficult to trace because they can be launched using a number of servers in different geographical locations.[61] The origins and the identity of the attackers are hidden as they find covert ways to gain access. More specifically, they use backdoor payloads to encrypt computers with malicious software and codes to attain access to those control systems.[62]

---

56 Jeff Melnick "Top 10 Most Common Types of Cyber Attacks" (15 May 2018) Netwrix <https://blog.netwrix.com>.

57 Francis Grimal and Jae Sundaram "Cyber Warfare and Autonomous Self-defence" (2017) 4 JUFIL 313 at 314.

58 Hathaway and others, above n 37, at 838.

59 Melnick, above n 56.

60 "Understanding Server Traffic logs and detecting Denial of Service Attacks" Microsoft <https://techcommunity.microsoft.com>.

61 Grimal and Sundaram, above n 57, at 315.

62 At 315.

2 Malware

A malware cyberattack is a malicious software that is installed into the computer programmes and networks of an unsuspecting user.[63] The malicious software embeds itself into a computer system and gains access to sensitive data.[64] It can be attached to a code by gaining physical access to the computer system, for example, by embedding the malicious code on a Universal Serial Bus Flash Drive (USB) and then plugging it into the computer's USB port.[65] It can also be embedded remotely by exploiting a vulnerability within the computer system.[66]

(a) Common forms of malware:

Malware can be launched in various forms including, worms and viruses. As Microsoft explains, a malware "is a catch-all term to refer to any software designed to cause damage to a single computer, server or computer network".[67] Below I will outline the most common forms of malware.

(i) Virus

A virus is a self-replicating malicious programme that infiltrates a computer system by attaching itself to a file or document.[68] It is programmed to infect computer servers and alter their operational features. This can result in damaged or deleted files, system failures, or loss of data.[69]

(ii) Worms

A worm is a malicious software that searches for vulnerabilities within the network, in order to replicate and reproduce itself across computer systems.[70] The worm can spread and replicate once a user downloads a compromised file or browses through a compromised website.[71]

---

63 Melnick, above n 56.

64 Josh Fruhlinger "Malware explained: How to prevent, detect and recover from it" (17 May 2019) CSO <www.csoonline.com> at 1.

65 At 2.

66 At 2.

67 At 2.

68 At 3.

69 Josh Fruhlinger "Viruses explained: How they spread and 5 signs you've been infected" (16 July 2019) CSO <www.csoonline.com>.

70 Melnick, above n 56.

71 Melnick, above n 56.

Unlike viruses, worms do not require a host file to replicate and spread across computer networks.

(ii) Ransomware

Ransomware targets a user's hard drive and takes control of its files, restricting the user's access to those files.[72] The malware notifies the user that they have been locked out of their files and that a sum of money must be paid to gain access to those files.[73] The user's access will only be regained once the payment has been made and the attacker gives up the decryption key to the files.[74] The motives of this malware are financial.

In this section I discussed the different interpretations of cyberspace, cyber-weapons and cyberattacks. This is a crucial first step toward analysing cyberattacks in the context of international law.

III Cyber Use of Force

Cyberattacks can vary in means and effects. This part will explain the limits of applying Article 2(4) UN Charter. It will focus on electoral interference and compare it to the Stuxnet cyberattack.

A Use of Force

Article 2(4) UN Charter sets out the prohibition against the use of force:[75]

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

72 Melnick, above n 56.

73 Fruhlinger, above n 64, at 4.

74 At 4.

75 Charter of the United Nations (opened for signature 26 June 1945, entered into force 24 October 1945), art 2(4).

The aim of those drafting the UN Charter was to "save succeeding generations from the scourge of war".[76] The principle to outlaw the threat or use of force remains at "the heart of the UN Charter".[77]

The term "use of force" is not defined by the Charter and its scope remains debated. The Charter's drafting history, followed by international declarations, judgments, state practice and scholarly examination, note that "force" is limited to "armed force".[78] Indeed, the *travaux préparatoires* made clear that political, psychological and economic forms of pressure did not fall within the scope of "force" under Article 2(4).[79] In fact, Brazil proposed adding economic coercion to the prohibition on the use of force in the UN Charter, but the proposal was rejected.[80] The 1970 General Assembly Declaration on Friendly Relations confirmed that "force" did not include political or economic coercion.[81] Thus, "force" strictly includes armed force, and not economic or political force.[82]

Finally, Article 2(4) explicitly prohibits a state from using force or threatening the use of force against another state's territorial integrity or political independence.[83] The Charter strengthens the prohibition by including a catch-all phrase "in any other manner inconsistent with the purposes of the United Nations".[84] The provision aims to preserve the territorial sovereignty, independence and equality of states.[85] The principle outlaws all inter-state uses of force or threat of force that may compromise the purpose of the United Nations.[86]

---

76 Catherine Lotrionte "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law" (2018) 3 CDR 78 at 78.

77 Louis Henkin "The Reports of the Death of Article 2(4) Are Greatly Exaggerated" (1971) 65 AJIL 544 at 544.

78 Tom Ruys *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge University Press, New York, 2010) at 7.

79 Lotrionte, above n 76, at 83.

80 Nils Melzer "Cyberwarfare and International Law" (02 November 2011) United Nations Institute for Disarmament Research <https://www.unidir.org> at 7.

81 *Special Committee on Principles of International Law concerning Friendly Relations and Co-operation among States* A/AC.125/SR.110 to 114 (1970); and *Report of the Special Committee on Friendly Relations and Co-operation among States* A/7326 (1969).

82 Roscini, above n 28, at 45.

83 Charter of the United Nations, art 2(4).

84 Charter of the United Nations, art 2(4).

85 Malcolm Shaw *International Law* (8th ed, Cambridge University Press, New York, 2017) at 857.

86 Richard Hanania "Norms Governing the Interstate Use of Force: Explaining the Status Quo Bias of International Law" (2013) 27 EL 831 at 840.

This section briefly explained the grounds of Article 2(4) UN Charter. In the next section I will point to the limitations of applying Article 2(4) in cyberspace.

B Can Article 2(4) UN Charter apply in Cyberspace?

The 2015 UNGGE consensus report affirmed that the prohibition of force applies to cyber-operations.[87] Article 2(4) UN Charter is concerned with the consequences of the operation rather than the instrument used to conduct the operation.[88] The prohibition, therefore, covers all instruments used by a state to commit an act resulting in death, damage or destruction.[89] For example, if State A launches a cyberattack against the power grid of State B, causing an intensive care unit to lose power, then that may amount to force under Article 2(4) UN Charter. Thus, "armed force" can include cyber-operations if it is used to conduct a hostile action, leading to destructive consequences.[90]

1 Three Approaches to Force

There are three main approaches that help explain the qualification of force. First, the instrument-based approach refers to the weapon used to conduct the operation.[91] In cyberspace, this approach would not be adequate in addressing cyber-threats as cyber-instruments are not comparable to traditional weapons.[92] Cyber-operations by their nature, would not amount to force under this approach because of their dual purpose of carrying out military and civilian functions. The International Court of Justice (ICJ) in the *Nuclear Weapons Advisory Opinion* affirmed that Article 2(4) applied to any use of force, regardless of the weapon used to carry out the attack.[93] Thus, the notion of force is not bound by its instrument.

---

87 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, above n 1, at 12.

88 Roscini, above n 28, at 50.

89 At 50. See Ian Brownlie *International Law and the Use of Force by States* (Oxford University Press, New York, 1963) at 362; and Ministry of Foreign Affairs and Trade (New Zealand) "The Application of International Law to State Activity in Cyberspace" (01 December 2020) New Zealand Foreign Affairs and Trade <www.mfat.govt.nz> at 2.

90 Russell Buchan "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" (2012) 17 JCSL 211 at 215.

91 François Delerue *Cyber Operations and International Law* (Cambridge University Press, Cambridge, 2020) at 289.

92 At 289.

93 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 at 22.

Second, the target-based approach focuses on the target of the operation.[94] In cyberspace the target-based approach would emphasise the cyber-operation's intended target, regardless of the effects or damage produced.[95] If a cyberattack targets and penetrates a nation's critical infrastructure, then that would satisfy Article 2(4) UN Charter.[96] However, this approach is too broad and subjective because there is no internationally agreed definition of what can qualify as "critical infrastructure".[97] This approach would also encompass minor disruptions, inconveniences and espionage operations.[98]

A strictly targeted-based approach means that cyber-operations aimed at gathering intelligence for national security purposes, will fall within the scope of force.[99] However, international law has not expressly outlawed the practice of intelligence gathering during peacetime. Moreover, states have not accepted cyber-espionage as a violation of force in international law.[100] For instance, in 2008, Russia embedded a malware on a USB and left it in the carpark of a United States military base.[101] An Official, picked up the USB and plugged it into the military's offline computer system.[102] The Operation, dubbed "Buckshot Yankee", allegedly allowed Russia to steal classified information from the United States Pentagon.[103] The United States responded by "supergluing" the USB port shut, and from what we know, they did not take any further action against the incursion.[104] Presumably, states and international legal forums have accepted cyber-espionage operations as part of their global affairs.[105]

94 Delerue, above n 91, at 289.

95 At 289. See Christopher Joyner and Catherine Lotrionte "Information Warfare as International Coercion: Elements of a Legal Framework" (2001) 12 EJIL825 at 855.

96 Roscini, above n 28, at 47.

97 At 47.

98 At 47.

99 Van de Velde, above n 45. See Walter Sharp *Cyberspace and the Use of Force* (Aegis Research Corporation, Virginia, 1999) at 130.

100 Russell Buchan *Cyber Espionage and International Law* (Oxford Hart Publishing, Oxford, 2019) at 68.

101 David Sanger, National Security Correspondent for New York Times (Michael Barbaro, The Daily Podcast, 16 December 2020).

102 Sanger, above n 101.

103 Gary Brown and Keira Poellet "The Customary International Law of Cyberspace" (2012) 6 SSQ 126 at 131.

104 Sanger, above n 101.

105 Tobias Kliem "You can't cyber in here, this is the War Room! A rejection of the effects doctrine on cyberwar and the use of force in international law" (2017) 4 RTFG 344 at 355.

Third, the consequence-based approach concerns the outcome of the operation.[106] It focuses on the consequences of the attack rather than the instrument or the target of the attack. Former State Department Legal Advisor, Harold Koh, claims that:[107]

> If the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force.

The international community accepts that large-scale cyberattacks unambiguously fall within the scope of Article 2(4) UN Charter.[108] This view is held by many states, including Australia, New Zealand, Finland, Germany, the Netherlands and Iran.[109] Therefore, under the consequence-based approach, cyberattacks which cause effects that resemble those of kinetic weapons will reach the threshold of force under Article 2(4).[110]

The Tallinn Manual elaborates on the consequence-based approach and adds that a "cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".[111] According to the Tallinn Manual, cyberattacks which cause injury, death or destruction, unquestionably falls within the scope of Article 2(4).[112] However, a small number of the Manual's authors concluded that the prohibition of force should be widely interpreted to include non-armed physical force.[113] For these authors,

---

106 At 347.

107 Michael Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" (2010) 54 HILJ 14 at 19.

108 Samuli Haataja and Afshin Akhtar-Khavar "Stuxnet and international law on the use of force: an informational approach" (2018) 7 CILJ 99 at 107.

109 Australian Government Department of Foreign Affairs and Trade "Australia's International Cyber Engagement Strategy" (October 2017) Australian Government Department of Foreign Affairs and Trade <www.dfat.gov.au> at 90. See also Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 3; Ministry of Foreign Affairs Finland "International law and cyberspace: Finland's national positions" (19 October 2020) Finnish Government <https://valtioneuvosto.fi> at 6; The Federal Government of Germany "On the Application of International Law in Cyberspace" (March 2021) Federal Foreign Office <www.auswaertiges-amt.de> at 6; Ministry of Foreign Affairs (Netherlands) "International Law in Cyberspace" Government of the Netherlands <www.government.nl> at 8; and "General Staff of Iranian Armed Forces Warns of Tough Reaction to any Cyber Threat" (18 August 2020) Nournews <https://nournews.ir>.

110 Roscini, above n 28, at 48.

111 Tallinn Manual, above n 13, at 45.

112 At 45.

113 Ryan Hayward "Evaluating the 'Imminence' of a Cyber Attack for Purposes of Anticipatory Self-Defense" (2017) 117 CLR 399 at 407.

causing the New York Stock Exchange to plummet would amount to an armed attack because the effects would be catastrophic to a nation's economy.[114]

In cyberspace, targeting the financial institutions of a state is a more likely scenario than targeting the power grid of a state and causing a nationwide power cut. For example, in 2017, the NotPetya ransomware attack, allegedly led by Russian officials, targeted corporate firms around the world. The attack cost Merck, a pharmaceutical company, USD 670 million.[115] Additionally, the WannaCry ransomware attack, allegedly orchestrated by the North Korean government, "affected between 230,000 and 300,000 computers in over 150 countries".[116] It is estimated that the attack had a cost consequence of USD 4 billion across the world, a financial consequence that impacted the globe.[117] Evidently, attacks of this nature may trigger a global financial crisis, leading to widespread unemployment or affect the public's confidence in the financial sector, causing widespread panic and uncertainty.[118]

2 The Consequence-based Approach

The most prominent violation of force in cyberspace occurred in 2010. In a joint effort with Israel, the United States began developing the "Olympic Games" cyber-weapon (also known as "Stuxnet").[119] The Stuxnet cyberattack was calculated to target Iran's Natanz uranium enrichment plant, specifically sabotaging its nuclear weapons programme.[120] It did this by speeding up and slowing down the rotation of its centrifuges, eventually leading to their break down.[121] The International Atomic Energy Agency (IAEA) who visited the plant to examine the centrifuges could not understand why the centrifuges were deteriorating at an alarming

---

114 At 407.

115 Kim Nash and others "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs" (27 June 2018) Wall Street Journal <www.wsj.com>.

116 Michael Schmitt and Sean Fahey "WannaCry and the International Law of Cyberspace" (22 December 2017) Just Security <www.justsecurity.org>.

117 Jonathan Berr ""WannaCry" ransomware attack losses could reach $4 billion" (16 May 2017) CBS News <www.cbsnews.com>.

118 Paul Mee and Til Schuermann "How a Cyber Attack Could Cause the Next Financial Crisis" (14 September 2018) Harvard Business Review <https://hbr.org>.

119 Kim Zetter *Countdown to Zero Day* (Crown Publishers, New York, 2014) at 194.

120 David E Sanger "Obama Order Sped Up Wave of Cyberattacks Against Iran" (01 June 2012) New York Times <www.nytimes.com>.

121 David Weissbrodt "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage" (2013) 22 NJIL 347 at 376.

rate.[122] The Stuxnet worm was stopped after it was discovered by VirusBlokAda, a Belarusian cybersecurity company.[123]

Iran was initially hesitant to confirm the attack but later acknowledged that an attack had taken place. [124] It subsequently announced that it was developing its own military cyber-unit.[125] It is also worth noting that Iran allegedly orchestrated the September 2012 DDoS cyberattacks against United States financial institutions as retaliation for the Stuxnet attack.[126]

Scholars, including those involved in the Tallinn Manual, have classified the Stuxnet malware as a use of force under Article 2(4) UN Charter.[127] Stuxnet began in the cyber-realm and caused real world physical effects to Iran's nuclear infrastructure.[128] Indeed, the malware reportedly destroyed 1000 of the 5000 centrifuges responsible for purifying Iran's uranium.[129] Arguably, the Stuxnet cyberattack crippled Iran's nuclear programme in a manner similar to that of a traditional weapon. Thus, the consequential outcome of the cyber-operations leads to a determination of force under Article 2(4) UN Charter.[130]

Nevertheless, most cyber-operations do not rise to that level of destruction. In particular, small-scale non-kinetic cyber-operations, which target and disrupt the economic and political structures of a nation, challenges the notion of armed force because of their limited physical effects.[131] For example, in 2016, the United States was experiencing a series of cyberattacks targeting its electoral processes. The Senate Intelligence Committee reported that Russian officials "were able to gain access to restricted elements of election infrastructure" and "were

---

122 Zetter, above n 119, at 2.

123 At 5.

124 Haataja and Akhtar-Khavar, above n 108, at 103.

125 Thom Shanker and David E Sanger "U.S. Suspects Iran Was Behind a Wave of Cyberattack" (13 October 2012) New York Times <www.nytimes.com>.

126 Nicole Perlroth and Quentin Hardy "Banking Hacking Was the Work of Iranians, Officials Say" (08 January 2013) New York Times <www.nytimes.com>.

127 Steve Ragan "Stuxnet Likely Constituted Illegal Act of Force, Study Says" (27 March 2013) Security Week <www.securityweek.com>. See Buchan, above n 90, at 214; Tallinn Manual, above n 13, at 45 and 58; and Kim Zetter "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'" (25 March 2013) Wired <www.wired.com>.

128 Weissbrodt, above n 121, at 376.

129 Sanger, above n 120.

130 Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 2. See also Ministry of Foreign Affairs Finland above n 109, at 6; Federal Government of Germany, above n 109, at 6. Ministry of Foreign Affairs (Netherlands), above n 109, at 4.

131 Kliem, above n 105, at 357.

in a position to, at a minimum, alter or delete voter registration data".[132] Russian military agents hacked into the servers of Hillary Clinton's presidential campaign and stole tens of thousands of confidential emails.[133] They launched a series of disinformation campaigns, creating and distributing divisive content online that would stoke fear, distrust and division among citizens.[134] Although Russia denies the claims, the attack was intended to undermine American democracy.[135] The cyberattack affected the United States capacity to conduct its election cycle free from influence, but it did not produce any physical damage.[136]

The 1970 General Assembly Declaration on Friendly Relations outlined the rights protected under Article 2(4) UN Charter:[137]

> 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 their right to self-determination and freedom and independence.

In international law, self-determination denotes that citizens have a right to freely decide, without foreign interference, on matters concerning their "political status and…their economic, social and cultural development".[138] The Declaration secured the rights of citizens to freely select their own government.[139]

Yet, it is argued that the 2016 Russian hacking of United States elections did not amount to force under the Charter because it did not result in physical damage. Seemingly, cyber-operations that cause minor physical damage may qualify as force, but cyber-operations that target and undermine the political infrastructure of a nation will not.[140] This raises questions regarding the scope of Article 2(4) and its failure to address the non-kinetic effects of cyber-

---

132 Abigail Abrams "Here's What We Know So Far About Russia's 2016 Meddling" (18 April 2019) Times <www.time.com>.

133 Nicholas Tsagourias "Electoral Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace" (26 August 2019) EJIL: Talk! <www.ejiltalk.org> at 8.

134 At 8.

135 Abrams, above n 132.

136 Tsagourias, above n 133, at 9.

137 *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States* [Declaration on Friendly Relations] GA RES 2625 XXV A/Res/2625 (1970).

138 International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976), art 1.

139 *Declaration on Friendly Relations*, above n 137.

140 Chris Kinslow "Game of Code: The Use of Force against Political Independence in the Cyber Age" (2018) 4 AL 29 at 31.

operations. For example, Stuxnet was classified as an illegal use of force in international law, despite having little effect in deterring Iran's nuclear programme.[141] Some experts estimate that Iran's nuclear programme was set back by two years, but a more accurate finding suggests that it was only set back by a few months.[142] Indeed, Iran was able to steadily recover its nuclear enrichment plants within months.[143]

In contrast, Russia's cyber-interference compromised the integrity of United States democratic institutions. As Arlen Printz points out:[144]

> Loss of confidence is especially significant in democratic forms of government which derive their legitimacy from their people's faith that the process accurately reflects the popular will.

Printz argues that launching a cyberattack to help support a particular candidate or to help shape a particular voting preference, or to simply undermine the political organisation of a state, can lead to long-term detrimental effects.[145] Citizens may choose to disengage or refrain from participating in the democratic process or question the legitimacy of the electoral process.[146]

This section intended to demonstrate the prohibition's inability to address the unique and dangerous consequences of non-kinetic cyber-operations. Indeed, repairing and restoring the public confidence in a nation's democratic process is much more difficult than repairing and restoring the centrifuges that were destroyed by the Stuxnet malware. Evidently, the prohibition's emphasis on physical severity excludes most cyber-operations that do not result in physical destruction, despite their damaging effects. The next section will evaluate whether the use of force is subject to a *de minimis* threshold of violence.

C De Minimis Force

141 Rebecca Slayton "Why Cyber Operations Do Not Always Favor the Offense" (February 2017) Harvard Kennedy School: Belfer Center for Science and International Affairs <www.belfercenter.org> at 4.

142 At 4.

143 At 4.

144 Arlen Printz "Election Hacking: Trifecta of Sovereignty, Intervention, and Use of Force Violations in International Law" (2019) 42 LLAICLR 308 at 313.

145 At 313.

146 At 312

The International Fact-Finding Commission on the Conflict in Georgia concluded that "the prohibition on the use of force covers all physical force which surpasses a minimum threshold of intensity".[147] That is, the use of force must meet a certain level of violence to qualify as force, violence that is minimal will not qualify as force under Article 2(4) UN Charter.[148]

Most scholars are in near consensus that Article 2(4) UN Charter must satisfy a *de minimis* threshold of violence to fall within the scope of *jus ad bellum*.[149] Anything below the threshold falls outside the prohibition of force.[150] In the context of cyberspace, the Tallinn Manual endorses a *de minimis* threshold of force and argued that trivial physical effects do not fall within the scope of Article 2(4) UN Charter.[151] It noted that "subject to a *de minimis* rule, consequences involving physical harm to individuals or property will in and of themselves qualify the act as use of force".[152]

The notion that the doctrine of force is subject to a minimum gravity threshold, poses further challenges in cyberspace. Cyber-operations operate differently from traditional kinetic attacks.[153] For instance, cyberattacks usually cause subtle long-term effects, absent of serious physical harm.[154] They aim to degrade and disrupt the social, economic and political institutions of a nation, actions which fall below the threshold of force.[155] Imposing a gravity threshold on the basis of physical effects limits the forcible legal recourse open to victim states that have been subject to a cyberattack.[156]

Legal scholar Tom Ruys rejects the notion that the prohibition of force is subject to a gravity threshold of violence.[157] He argues that the prohibition of force is not limited to large-scale

147 Lotrionte, above n 76, at 84.
148 Ruys, above n 2, at 159.
149 Mary Ellen O'Connell "The True Meaning of Force: A Further Response to Tom Ruys in the Interest of Peace" (2014) 108 ASIL 153 at 154. See Lotrionte, above n 76, at 84; and Olivier Corten *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart Publishing, London, 2010) at 69.
150 Ruys, above n 2, at 159.
151 Delerue, above n 91, at 296.
152 Tallinn Manual, above n 13, at 48.
153 Sarah Kreps and Jacqulyn Schneider "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics" (2019) 5 JCS 1 at 1.
154 Printz, above n 144, at 310.
155 At 311.
156 Kreps and Schneider, above n 153, at 2.
157 Ruys, above n 2, at 159.

forcible action. Ruys finds that "excluding small-scale or 'targeted' forcible acts from the scope of Article 2(4) is inconsistent with customary practice".[158] He adds that small-scale unlawful incursions can amount to force, even if they do not result in direct confrontation.[159] Indeed, foreign agents who intentionally and repeatedly enter into the territory of another state, violating its sovereignty, may violate Article 2(4) UN Charter.[160] However, small-scale incursions are subject to hostile intent.[161] For example, there are instances that would not amount to force, including military personnel accidentally crossing onto the territory of another state, or an aircraft making an emergency landing onto foreign territory to avoid crashing.[162] Here, the missing component is hostile intent.[163] While this determination can be subjective in cyberspace, hostile intent ensures that acts which are innocuous or accidental, are excluded from Article 2(4).[164]

However, Ruys recognises that "incursions that are initially harmless may gradually come to display hostile intent".[165] For instance, repeated trespass against a nation's territory may amount to force if it is carried out by an adversary state near a restricted area.[166] In such a scenario, defensive force would not be permitted. Instead, the victim state would order the withdrawal of state agents from is territory.[167] However, if state agents continue to intrude, ignoring the requests of the victim state and undermining its sovereignty, then subject to the elements of necessity and proportionality, limited defensive force should be available to the victim state.[168] This was evidenced during the Cold War, when the Soviet Union shot down U-2, an American spy plane flying over Soviet territory.[169] The Soviet Union deemed the response necessary,

158 At 159.

159 At 171. See also Agata Kleczkowska "When 'the Use of Force is Prohibited? – Article 2(4) and the 'Threshold' of Use of Force" (2019) 8 AMULR 110 at 111.

160 Ruys, above n 2, at 189. See generally Claus Kress "On the Principle of Non-Use of Force in Current International Law" (30 September 2019) Just Security <www.justsecurity.org>.

161 At 173.

162 At 173.

163 At 173.

164 At 173.

165 At 173.

166 At 173.

167 At 173.

168 At 173.

169 Department of United States of America "U-2 Overflights and the Capture of Francis Gary Powers 1960" Office of the Historian Office of the Historian <https://history.state.gov>.

citing the repeated and deliberate nature of the incursion.[170] States, including the United States, did not condemn Soviet action as illegal under international law.[171]

Nonetheless, qualifying the repeated incursion of cyber-infrastructures as a "use of force" may be a broad interpretation of Article 2(4). Indeed, the borderless and interconnected nature of cyberspace means that states are dependent on the cyber-networks of other states to conduct their day-to-day functions.[172] However, the requirement of hostile intent may help distinguish lawful from unlawful incursion in cyberspace. For example, a state may use the cyber-infrastructure of another state to send an email. This would not be classified as unlawful incursion amounting to force because there is no hostile intent to disrupt the ordinary functions of the computer network. Sending an email is considered an ordinary and proper function of cyberspace. On the other hand, if a state knowingly sends a number of emails, embedded with a malicious software, then that may amount to unlawful incursion. The difference is the hostile intention to send an email that may disrupt and interfere with the functioning of a state's computer network.

Finally, Ruys determines that a threshold of force does exist, but it is not as high as the current international law suggests.[173] Ruys outlines several factors that may guide the decision of states to respond using force: the geopolitical relationship between the states involved; the location of where the intrusion occurred; and the repeated attempts to intrude.[174] Hence, I consider that the intent of the intruding state, the location of the intrusion and the repeated efforts to intrude, to be relevant considerations in the context of cyberspace.[175] I argue that repeatedly launching small-scale cyber-operations against the critical functions of a state, is a violation of Article 2(4) UN Charter.

---

170 Ruys, above n 2, at 174.

171 At 174

172 Tsagourias, above n 6, at 13.

173 Ruys, above n 2, at 208. See generally Eliav Lieblich "The Salisbury Incident and the Threshold for "Unlawful Use of Force" under International Law: between Stigmatization and Escalation" (20 April 2018) Stockholm Centre for the Ethics of War and Peace <http://stockholmcentre.org>; Dapo Akande "The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?" (17 March 2018) EJIL Talk! <www.ejiltalk.org>.

174 Ruys, above n 2, at 175.

175 At 175-176.

To illustrate, after the 2016 hacking, Russia allegedly attempted to penetrate Illinois' voter registration database to access voter registration records.[176] While it made no attempt to delete or alter voter data, it demonstrates Russia's willingness to repeatedly intrude and undermine the territorial sovereignty of the United States. In 2020, once again, Russia allegedly attempted to compromise the United States democratic processes by targeting political parties and campaigns.[177] Russia's repeated efforts to hack into the electoral functions of the United States may be classified as unlawful incursion. Their intention to undermine the political independence of the United States may lead to a qualification of force.[178]

States have previously been willing to take forcible action in response to small-scale unlawful incursions. Accordingly, the threshold of force under Article 2(4) is not as high as the international legal framework suggests. We should be wary when trying to enforce such a threshold in cyberspace.

This Chapter examined the traditional notions of force and pointed to its limitation in cyberspace. The following Chapter will discuss the need to apply a new approach in cyberspace.

IV New Approach to Force in Cyberspace

Most cyber-operations target governmental and financial networks, causing data destruction or disruption of services.[179] They can destabilise computer systems without physically destroying them.[180] Therefore, when examining severity, it may be worth considering the nature of the target, namely, whether a cyberattack targeted the critical infrastructure of a state. This approach may represent a starting point for cyberattacks that do not result in physical consequences but are condemned under Article 2(4) UN Charter.

176 United States Senate Intelligence Committee "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election" (25 July 2019) U.S. Senate Select Committee on Intelligence <www.intelligence.senate.gov> at 22.

177 Kari Paul "Russian hackers targeting US political campaigns ahead of election, Microsoft warns" (10 September 2020) The Guardian <www.theguardian.com>.

178 Kinslow, above n 140, at 30. See Printz, above n 144, at 314. But see Ryan Goodman "International Law and the US Response to Russian Election Interference" (05 January 2017) Just Security <www.justsecurity.org>.

179 Delerue, above n 91, at 297.

180 At 297.

A Target and Consequence

In the context of cyberspace, a strictly consequence-based approach cannot meet the complex effects of cyber-operations that do not result in loss of life, injury or damage to property.[181] Instead, a target-based approach must supplement the consequence-based approach. That is, the target of the operation, combined with its effects, will help determine whether a cyber-operation amounts to force.[182] Namely, a cyberattack which targets a state's critical infrastructure and causes non-destructive effects, may still qualify as a use of force.[183]

A state's critical infrastructure is managed by computer control systems and networks, making it highly susceptible to cyberattacks.[184] The 2021 UNGGE report recognised this and emphasised the importance of protecting critical infrastructure from cyberattacks:[185]

> States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public.

The Report warned against cyberattacks that target critical infrastructure:[186]

> States should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Under the proposed approach, a cyber-operation must target the critical infrastructure of a nation, rendering it ineffective to carry out its programmed functions.[187] For example, in 2007,

---

181 At 304.

182 At 304. See Roscini, above n 28, at 58; Brown and Poellet, above n 103, at 137; William Owens and others *Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press, Washington D.C, 2009) at 254.

183 Michael N Schmitt Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017) [Tallinn Manual 2.0] at 343.

184 Delerue, above n 91, at 303.

185 *Open-ended working group on developments in the field of information and telecommunications in the context of international security* A/AC.290/2021/CRP.2 (2021).

186 *Open-ended working group on developments in the field of information and telecommunications in the context of international security*, above n 185.

187 Nicholas Tsagourias "Cyber Attacks, Self-defence and the Problem of Attribution" (2012) 17 JCSL 229 at 231.

Russia allegedly launched a series of cyberattacks, targeting Estonia's critical infrastructure.[188] The DDoS cyberattacks caused widespread disruption as Estonians could not access essential sectors, including governmental websites and banking services.[189] In 2015, Ukraine's power grids were hit by a cyberattack which caused a widespread power outage affecting more than 200,000 people.[190] Launching such an attack against a nation's critical infrastructure may tip the scale towards a qualification of force, even if its effects are non-destructive.[191] The target of the operation is a relevant factor in assessing the effects of the cyber-operation.

Unlike other states, France acknowledged the target-based approach and declared that low-intensity cyber-operations that do not result in physical effects may still qualify as force.[192] It added that the applicability of force will be determined by, but not limited to:[193]

- The circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not);
- The extent of intrusion;
- The actual or intended effects of the operation; and
- The nature of the intended target.

France explained that penetrating its critical infrastructure, namely, its military systems, to obstruct its defence capabilities, may amount to force under the Charter.[194] According to France, the target of the operation may support a finding of force under Article 2(4).[195]

Although this may create a legal grey area for attacks that do not target critical infrastructure, it may help address cyber-operations that threaten international peace and security, despite their limited physical consequences. However, accepting this approach will require a globally

188 Tamkin, above n 35.

189 Tamkin, above n 35.

190 Donghui Park and others "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks" (11 October 2017) The Henry M. Jackson School of International Studies: University of Washington <https://jsis.washington.edu>.

191 Delerue, above n 91, at 298.

192 Ministry of Armed Forces (France) "International Law Applied to Operations in Cyberspace" (October 2019) Ministère des Armées <www.defense.gouv.fr> at 7.

193 At 7.

194 Przemyslaw Roguski "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part II" (24 September 2019) Opinio Juris <http://opiniojuris.org>.

195 Roguski, above n 194.

recognised definition of what will qualify as critical infrastructure.[196] This will help eliminate the subjective assessment of what may qualify as critical infrastructure between states.

B Global Definition of Critical Infrastructure

Currently, there is no internationally accepted definition of critical infrastructure and how it is defined will vary between states.[197] Nonetheless, most states share a similar definition of what constitutes "critical infrastructure". In 2017, the United Kingdom defined it as:[198]

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

Similarly, France designated 12 sectors as critical infrastructures:[199]

- Government (civilian activities of the State; military activities of the State; judicial activities; space and research).
- Protection of the population (health; water supply; food supply).
- Economic and social sectors (energy; information, audio-visual and electronic communications; transport; finance; industry).

In 2003, a UN General Assembly Resolution concerning the *Creation of a Global Culture of CyberSecurity and the Protection of Critical Information Infrastructures* stated that critical infrastructure includes but is not limited to, the "transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food

196 Colleen Newbill "Defining Critical Infrastructure for a Global Application" (2019) 26 IJGLS 761 at 764.
197 At 768.
198 At 770.
199 Delerue, above n 91, at 301.

distribution and public health".[200] Thus, the wider international community agrees that critical infrastructure is made up of agencies and institutions that are vital to state functioning and its protection against cyberattacks is therefore fundamental.

Recent events suggest that a state's electoral functions are becoming a more likely target in cyberspace. The 2021 UNGGE Report correctly noted that cyber-interference of political processes was becoming a "real and growing concern."[201] It is, therefore, important to consider whether electoral processes may qualify as critical infrastructure under international law. International cyber-norms award critical infrastructure with special protection. Some states have sought to determine whether that protection can extend to electoral infrastructures, or more specifically, whether the democratic infrastructure of a nation can qualify as critical infrastructure.

Under the targeted-consequence-based approach, the election infrastructure of a nation must be designated as a protected entity of a nation's critical infrastructure. As Printz recognises:[202]

> … the nature of the attack, the nature of the targets, (in this case an attack on a State's Critical Infrastructure, that usurps an essential State function), and the severity of the consequences of assaulting a State's very political independence, customary international law's prohibition of the use of force should at a minimum be read to include election hacking.

Defining electoral infrastructure as "critical infrastructure", will help affirm the integrity of the electoral process against foreign cyber-interference and enhance the democratic foundations of a nation.[203]

Prior to the 2016 Russian hacking, the United States National Strategy to Secure Cyberspace outlined that critical infrastructure included both public and private sectors that were essential to the functioning of a state. It made no mention of electoral institutions.[204] After the Russian

---

200 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, GA Res 58/199, A/RES/58/199 (2004).

201 *Open-ended working group on developments in the field of information and telecommunications in the context of international security*, above n 185.

202 Printz, above n 144, at 314.

203 At 313.

204 Department of Homeland Security "The National Strategy to Secure Cyberspace" (February 2003) Cybersecurity and Infrastructure Security Agency <https://us-cert.cisa.gov>.

cyber-hacks, the Department of Homeland Security (DHS) announced that federal election infrastructure would form part of United States critical infrastructure.[205] DHS Secretary Jeh Johnson explained that "election infrastructure" included:[206]

> Storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

The DHS acknowledged that the United States electoral process was highly dependent on cyber-networks, making it more vulnerable to cyberattacks. The designation intends to prioritise and protect United States electoral functions within its National Infrastructure Protection Plan.[207]

The Global Commission on the Stability of Cyberspace (GCSC), a non-government organisation, sponsored by Switzerland, Japan and Estonia, established a number of norms pertaining to cyberspace.[208] In its 2019 Report, it labelled the electoral functions of a nation as "critical", and developed a new set of international norms against cyber-interference of election infrastructure.[209] The Report confirmed that launching a cyberattack to manipulate the electoral process of a nation was impermissible, regardless of whether it can be viewed as a "violation of international law or not".[210] It concluded that "state and non-state actors must not pursue, support or allow cyber-operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites".[211]

---

205 Brian Humphreys "The Designation of Election Systems as Critical Infrastructure" (18 September 2019) Congressional Research Service <https://crsreports.congress.gov>.

206 Jeh Johnson "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector" (06 January 2017) Homeland Security <www.dhs.gov>. See generally Kristen Eichensehr "Political Parties as Critical Infrastructure?" (22 June 2017) Just Security <www.justsecurity.org>.

207 Johnson, above n 206.

208 "Advancing Cyber Stability" (November 2019) Global Commission on the Stability of Cyberspace <https://cyberstability.org> at 20.

209 At 20.

210 At 33.

211 At 33.

Nevertheless, establishing a global definition of "critical infrastructure" will be difficult.[212] Certainly, how the global community defines "critical infrastructure" will depend on the priorities of each state.[213] Nations that hold democratic elections will more likely support an inclusion of "election infrastructure" in its broader global definition. They may be more willing to support efforts that enhance their election security. On the other hand, nations that do not hold democratic elections and are usually the aggressors of cyber-election hacking, will be more reluctant to establish such a definition.[214]

C Cyber-Intervention

This section will examine the principle of non-intervention in accordance with cyber-disinformation. It will attempt to provide an alternative to compulsion in cyberspace.

1 Principle of Non-Intervention

Article 2(1) of the UN Charter acknowledges that state sovereignty and sovereign equality are foundational principles in international law.[215] States have the authority to legislate and enforce their own rules within their territory.[216] This principle of sovereignty gives rise to the principle of non-intervention which protects and upholds the right of states to govern freely from outside interference.[217]

The ICJ in *Nicaragua* discussed the principle of non-intervention. There, the United States was found to be in breach of the principle of non-intervention after funding and training the Contra

---

212 David Fidler "Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection" GJLA (2015) 8.

213 Newbill, above n 196, 764.

214 Louk Faesen and others "Case Study: Protecting Electoral Infrastructure from Russian Cyberoperations (2020) HCSS 16 at 24.

215 Przemyslaw Roguski "Violation of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach" Dennis Broeders and Bibi van den Berg (ed) *Governing Cyberspace Behaviour, Power, and Diplomacy* (Rowman & Littlefield Publishers, London, 2020) 65 at 70.

216 At 70.

217 Sean Watts "Low Intensity Cyber Operations and the Principle of Non-Intervention" 14 (2014) BYIL 137 at 139.

rebel group to fight against the Sandinista government of Nicaragua.[218] The Court explained that the principle of non-intervention:[219]

> … forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy.

The court drew on the 1970 General Assembly Declaration on Friendly Relations which imposed an obligation on states to refrain from intervening in the domestic affairs of another state.[220] Thus, for foreign interference to qualify as unlawful intervention, it must interfere with a state's right to govern and decide freely over its territory and domestic jurisdiction.[221] It must target the *domaine réservé* of the victim state.

Initially, the borderless and infinite nature of cyberspace may challenge the notion of territory and sovereignty characterised by the principle of non-intervention. However, the 2015 UNGGE consensus report concluded that cyber-infrastructures which are located within the territory of a state fall within the prerogative powers of that state.[222] States have affirmed this by taking measures to secure their cyber-infrastructures and by sanctioning those who have maliciously penetrated their computer networks.[223]

The report also clarified that the principle of non-intervention applies in cyberspace.[224] It has become increasingly clear that most cyber-operations will target the economic and political institutions of a state without the use of force. While these operations can have detrimental effects on a nation's stability, they will not have physically destructive effects.[225] Cyber-

---

218 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14 [Military and Paramilitary Activities] at 166.

219 At 167.

220 *Declaration on Friendly Relations*, above n 137.

221 *Military and Paramilitary Activities*, above n 218, at 165.

222 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, above n 1, at 12.

223 Roguski, above n 215, at 72

224 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, above n 1, at 12.

225 Christian Henderson "The use of cyber force: Is the jus ad bellum ready?" (2016) 27 QIL 3 at 3.

operations that do not violate the principle of force, may violate the principle of non-intervention.[226]

2 Cyberspace Coercion

Under the principle of non-intervention, a foreign state must do more than merely intrude into the territory or sovereignty of another state. The foreign state must coercively intervene in the internal and external affairs of another state.[227] The court in *Nicaragua* added that:[228]

> Intervention is wrongful when it uses, in regard to such choices, methods of coercion, particularly force, either in the form of military action or in the indirect form of support for subversive activities in another State.

Coercion is "the essence of intervention".[229] The perpetrating state must compel or pressure the victim state to take a particular action.[230] For state behaviour to be coercive, it must impede the ability of the victim state to exercise its own sovereign affairs.[231] The perpetuating state demands that the victim state alter its policy, regardless of whether the advantage sought by the perpetrating state is achieved.[232]

It may be suggested that the principle of non-intervention is out of date and does not extend to coercive cyber-operations.[233] The ICJ did not define coercion in great detail, but the 1976 Declaration on Non-interference described coercive measures as:[234]

> All forms of overt, subtle and highly sophisticated techniques of coercion, subversion and defamation aimed at disrupting the political, social or economic order of other States or destabilizing the Governments seeking to free their economies from external control or manipulation.

---

226 Watts, above n 217, at 146.

227 At 146.

228 *Military and Paramilitary Activities*, above n 218, at 165.

229 Id Kilovaty "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information" (2018) 9 HNSJ 146 at 168.

230 Harriet Moynihan "The Application of International Law to Cyberspace: Sovereignty and Non-intervention" (13 December 2019) Just Security <www.justsecurity.org> at 4.

231 Thibault Moulin "Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward" (2020) JCSL 1 at 18.

232 At 22.

233 Roscini, above n 28, at 64.

234 *Non-interference in the internal affairs of States* GA Res 31/91, A/31/414 (1976).

Therefore, coercion includes cyber-operations that are launched to control and apply pressure on another state.[235]

Nonetheless, the unlawful cyber-tactics conducted by states often fail to satisfy the element of coercion required by the principle of non-intervention.[236] More specifically, disinformation campaigns that spread "false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit" fail to fall within the scope of non-intervention.[237] The element of coercion is usually absent in most disinformation campaigns because they do not violate the free will of the target state.[238] Instead, they interfere in the affairs of a state by attempting to influence or persuade public opinion.[239]

To demonstrate, Russia's alleged hacking in 2016 violated the right of the United States to conduct its elections without foreign interference.[240] However, the 2016 hacking did not violate the principle of non-intervention because it lacked the coercive methods required under *Nicaragua*.[241] Although Russian hackers harmed Hillary Clinton's presidential run by spreading anti-Clinton propaganda across various social media platforms, they did not coerce citizens into voting for a particular candidate.[242] Their attempts to distribute divisive content online may have influenced citizens to vote for a particular candidate, but it did not coerce them into doing so. Coercion would apply if Russian officials had deleted registered voters or blocked voting machines, thus preventing people from voting.[243] The hack-and-leak operations did not fundamentally subordinate the independence of the United States.

235 Roscini, above n 28, at 64.

236 Moulin, above n 231, at 2.

237 European Commission "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation" (March 2018) Publication Office of the EU <https://op.europa.eu> at 3.

238 Tsagourias, above n 133, at 7.

239 At 7.

240 At 10.

241 Moulin, above n 231, at 2. See also Tsagourias, above n 133, at 6; and Jens Ohlin "Did Russian Cyber Interference in the 2016 Election Violate International Law?" (2017) 95 TLR 1580 at 1594.

242 Kilovaty, above 229, at 150.

243 Tsagourias, above n 133, at 10.

Traditional notions of coercion fail to acknowledge the weaponisation of cyberspace and its effects.[244] Indeed, it is concerning that a coordinated and organised effort to release a flood of disinformation in order to manipulate the electorate to vote in a particular way does not breach the rule of non-intervention. Legal scholar Sean Watts argues that the boundaries of coercion do not appropriately translate in cyberspace.[245] He adds that a re-examination of the law is required to address the novel effects produced by cyberspace. Watts suggests that coercion should be determined by: [246]

> The nature of state interests affected by a cyber operation, the scale of effects the operation produces in the target state, and the reach in terms of number of actors involuntarily affected by the cyber operation in question.

The principle of non-intervention should focus on the operation's attempt to "affect the protected state interests and the effects that such an operation produces".[247] The state has an interest in preserving the integrity of its election infrastructure and democratic processes. Undermining the decision-making powers of its electorates will compromise the efficiency, effectiveness and legitimacy of democratic elections.[248] The argument posed by Watts may help address operations that lack compulsion but work to sway or shape public opinion.

3 States on Disinformation

Disinformation has become a topical issue as the political affairs of states continue to be undermined in cyberspace. Yet, states have not developed a clear set of international norms concerning foreign intervention in the form cyber-disinformation.[249] While government officials have raised the issue of cyber-disinformation, many have declined to identify the rule violated under international law or have been reluctant to apply the principle of non-intervention. For example, in 2011, the Shanghai Cooperation Organization (SCO), comprised of China, Russia, Kazakhstan, Tajikistan, and Uzbekistan, submitted an International Code of

244 Kilovaty, above 229, at 171. See Henning Lahman "Information Operations and the Question of Illegitimate Interference under International Law" (2020) 53 ILR 189 at 210; Ohlin, above n 241, at 1593.

245 Watts, above n 217, at 146.

246 At 146. See Kilovaty, above n 229, at 171.

247 Kilovaty, above n 229, at 171.

248 At 171.

249 Buchan, above n 90, at 224.

Conduct to the UN Secretary-General.[250] The Code concluded that states must not use information and communication networks to "interfere in the internal affairs of other states or with the aim of undermining their political, economic and social stability". [251] The statement did not expressly point to the principle of non-intervention but asserted that international law must deter cyber-techniques aimed at undermining the political stability of a nation.[252]

More recently, Iran released its national statement concerning the role of international law in cyberspace. The statement examines the principle of non-intervention and notes that:[253]

> Measures like cyber manipulation of elections or engineering the public opinions on the eve of the elections may be constituted of the examples of gross intervention. … Cyber activities paralyzing websites in a state to provoke internal tensions and conflicts or sending mass messages in a widespread manner to the voters to affect the result of the elections in other states is also considered as the forbidden intervention.

Iran is silent on the matter of coercion and did not express in clear terms that cyber-manipulation by way of disinformation can fall within the boundary of coercion.[254] Accordingly, it is unclear whether Iran considers intervention in its electoral affairs to be inherently coercive or whether such interference may be coercive in limited circumstances.[255] Nonetheless, Iran's official statement is noteworthy because it establishes a legal boundary on a topical issue. It argues that cyber-campaigns which are designed to manipulate the democratic processes of a state may breach the principle of non-intervention.[256]

Iran's reference to foreign influence as a potential breach of non-intervention is shared by other western democracies, including Australia, the United Kingdom and the United States.[257] For instance, in 2017, the Prime Minister of Australia stated that "foreign powers are making

---

250 *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* GA Res 69/723, A/69/723 (2015) at 1.

251 At 5.

252 Kilovaty, above n 229, at 164.

253 "General Staff of Iranian Armed Forces Warns of Tough Reaction to any Cyber Threat," above n 109.

254 Przemyslaw Roguski "Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace" (03 September 2020) Just Security <www.justsecurity.org>.

255 Roguski, above n 254.

256 Roguski, above n 254.

257 Roguski, above n 254.

unprecedented and increasingly sophisticated attempts to influence the political process, both here and abroad".[258] George Brandis, former Attorney-General of Australia, echoed the Prime Minister's concerns and noted that "covert foreign influence can cause immense harm to our national sovereignty, to the safety of our people, to our economic prosperity, and to the very integrity of Australian democracy".[259] As a result, Australia added to its previous national statement and concluded that:[260]

> A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state's economic, political, and social systems, and foreign policy.

Accordingly, coercion is not limited to compulsion; coercion can include other forms of indirect conduct.[261] It can include operations that impede the ability of the victim state to exercise effective "control over its sovereign function".[262] Therefore, cyber-enabled disinformation that serves to manipulate electoral decision-making, may violate the principle of non-intervention.[263]

In contrast, the Netherlands recognised that the advancement of information technology "has given states more opportunities to exert influence outside their own borders and to interfere in the affairs of other states".[264] They outlined that foreign actors using various social media platforms "to influence election outcomes" is one example of that interference. However, the government emphasised the need for compulsion and explained that:[265]

> The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law. In essence it means compelling a state to take a course of action (whether an act or omission) that it would not otherwise

258 Lahman, above n 244, at 212.
259 At 212.
260 "2019 International Law Supplement" (2019) Australia's International Cyber Strategy <www.dfat.gov.au>.
261 Harriet Moynihan "The vital role of international law in the framework for responsible state behaviour in cyberspace" (2020) JCP 1 at 10.
262 At 11.
263 At 11.
264 Roguski, above n 254.
265 Moynihan, above n 161, at 10.

> voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state.

The action taken by the foreign actor must drive the victim state to alter its policy or change its behaviour.[266] The Netherlands are unique in that they take a very conventional approach to coercion in cyberspace.[267]

Other democratic nations have been reluctant to legally condemn cyber-disinformation as a violation of non-intervention.[268] They cite the need to preserve freedom of expression and the free flow of information sharing.[269] They fear that such measures may legitimise authoritarian practices of silencing dissidents and activists.[270] For instance, Egypt, Indonesia and Kuwait have all implemented domestic legislation that criminalises cyber-disinformation, however, they do not differentiate between foreign actors and domestic actors.[271] Indeed, laws that are designed to target foreign disinformation, may be disguised to supress the speech of the masses.[272]

Interestingly, New Zealand may classify an operation of disinformation as a violation of the principle of non-intervention.[273] In its national statement, it endorses the *Nicaragua* test of non-intervention and provides examples of when such a violation may occur:[274]

- A cyber operation that deliberately manipulates the votes tally in an election or deprives a significant part of the electorate of the ability to vote: or
- Prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic.

Thus, New Zealand accepts that a long series of disinformation campaigns may violate the principle of non-intervention. However, the statement does not express in certain terms whether a disinformation operation to undermine New Zealand's electoral process will violate that

266 At 10

267 Michael Schmitt "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis" (14 October 2019) Just Security <www.justsecurity.org>.

268 Roguski, above n 254.

269 Roguski, above n 254.

270 Lahman, above n 224, at 213.

271 At 213.

272 At 213.

273 Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 2.

274 At 2.

principle of non-intervention. It appears that New Zealand is also reluctant to accept foreign influence of democratic processes as non-intervention.

It is important to ensure that the international legal framework does not limit the rights and freedoms of citizens in cyberspace. However, our understanding of coercion fails to capture the unique characteristics and effects of cyber-operations. Foreign interference through disinformation can have exponential consequences on a nation's democracy and we must establish norms against interference.

Finally, it must be noted that before any forcible action can be taken, a cyberattack must be attributed to a state. Since cyberspace is accessible and can be used by individual members or groups, the next chapter aims to examine the role of state responsibility.

V Attribution in Cyberspace

To hold a state accountable under international law, the victim state must ascertain responsibility under the law.[275] This Chapter aims to explain the difficulties of attribution in cyberspace and outlines the standard of proof required to establish attribution.

A Attribution

The international principles governing attribution are defined in the International Law Commission's (ILC) Articles on State Responsibility (ARSIWA). According to Article 2 ARSIWA, there are two elements that must be satisfied when determining international responsibility:[276]

> There is an internationally wrongful act of a State when conduct consisting of an action or omission:
>
> (a) is attributable to the State under international law; and
>
> (b) constitutes a breach of an international obligation of the State.

---

275 Aravindakshan, above n 4, at 286.

276 *Responsibility of States for Internationally Lawful Acts (Commentary)* GA Res 56/83, A/Res/56/83 (2001) [Draft Articles] at 34.

In the context of cyberspace, attribution is more complex than usual. More specifically, it is difficult to ascertain responsibility when computers are generally accessible to ordinary individuals around the world. An individual can misuse cyberspace and launch a cyberattack through mere access to "a computer, software and a connection to the internet".[277] In recent years, the world has witnessed a number of patriotic hackers, carrying out cyberattacks in pursuit of political and financial gain.[278] This was evident in 2008, when pro-Russian hackers carried out a series of DDoS cyberattacks, targeting Georgia's government servers, media websites and financial institutions.[279] This raises the question of when a state can be held responsible for the private actions of an individual. This section is concerned with private actors who hack and launch cyberattacks against state adversaries, in the name of patriotism.[280]

International law would not expect a state to be responsible for all the actions taken by private individuals within its jurisdiction. In *United States Diplomatic and Consular Staff in Tehran*, Iranian demonstrators seized the United States Embassy and held consular officials hostage.[281] The ICJ explained that the initial siege conducted by Iranian students, could not be attributed to the state of Iran.[282] However, once Ayatollah Khomeini "endorsed" the occupation, the actions of the students became actions of the state.[283] The ICJ noted that the endorsement was verbally expressed by the highest authority of the state, which turned the "continuing occupation of the Embassy and detention of the hostages into acts of that State".[284] Iran assumed responsibility when it failed to adequately protect the Embassy from occupation.[285] The ICJ also pointed to Iran's "inaction", arguing that Iran failed to take "appropriate steps" to end the occupation.[286]

277 Marco Roscini "World Wide Warfare – Jus ad Bellum and the Use of Cyber Force" 14 MPYUL (2010) 86 at 97.

278 Paulo Shakarian "The 2008 Russian Cyber-Campaign Against Georgia" (2011) Military Review 63 at 64.

279 At 64.

280 At 64.

281 *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) (Judgment)* [1980] ICJ Rep 3 at 5.

282 At 35.

283 At 35.

284 At 35.

285 At 12.

286 At 31 – 32.

Article 11 ARSIWA outlined the rules of state attribution of private acts:[287]

> Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

The commentators explained that the state must acknowledge and adopt the wrongful conduct "as its own".[288] They add that "mere support or endorsement" of wrongful conduct, is not sufficient for attribution.[289] The ILC recognised that the ICJ in *United States Diplomatic and Consular Staff in Tehran*, had used words like "approval" and "endorsement" to attribute responsibility, but noted that this was "sufficient in the context of that case".[290] The commentators clarified that "conduct will not be attributable to a State under Article 11 where a State merely acknowledges the factual existence of conduct or expresses its verbal approval of it".[291] The state must demonstrate "clear and unequivocal" acknowledgement of the wrongful violation. This may be express verbal approval or inferred by the behaviour of the state.

Although "mere endorsement" may not be enough to show attribution, it may be enough to show that the state allowed its territory to be used to harm another state.[292] In *Corfu Channel,* the court held that a state should not "knowingly allow its territory to be used for acts contrary to the rights of other states".[293] This was also confirmed by the 2015 UNGGE Report.[294] However, this duty of due diligence to ensure that cyberattacks are not developed and launched from within the territory of a particular state, places a heavy burden on those states that are not technologically advanced. Indeed, cyber-weapons are easily accessible and are difficult to detect and trace, in contrast to traditional weapons which are easily traceable and cannot be accessed by ordinary citizens. The UNGGE acknowledged that:[295]

---

287 Draft Articles, above n 276, at 52.

288 At 53.

289 At 53.

290 At 53.

291 At 53.

292 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania) (Merits)* [1949] ICJ Rep 3 at 22.

293 At 22.

294 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* above n 1, at 8.

295 At 8.

> While such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity.

Therefore, I uphold the due diligence standard shared by New Zealand, that a state must have actual knowledge of the malicious cyber-operation and must "take reasonable steps within their capacity" to end the malicious activity.[296] It must do all it can to end the malicious cyber-activity.[297]

States enjoy the anonymity of cyberspace and are unlikely to pursue express public approval and acknowledgment of cyberattacks. Turning again to the Russia-Georgia cyber-conflict, pro-Russian patriotic hackers allegedly published instructions on how to conduct DDoS cyberattacks against Georgia. The website "StopGeorgia.ru", was launched to psychologically injure the Georgian population and support Russia's armed confrontation with Georgia.[298] The Kremlin did not publicly embrace or endorse the actions of the individuals.[299] However, Russia failed to exercise its due diligence in preventing and mitigating the attacks. The Kremlin also refused to cooperate with Georgian investigators.[300]

Once a state has been made aware of a cyberattack, it must take the necessary measures required to prevent or halt any incoming attack. This could include restricting the internet access of those individuals or enhancing its firewall network to monitor online traffic.[301] Thus, assuming in the case of the Russia-Georgia cyber-conflict that the hackers were indeed Russian patriots, responsibility for their actions could be imputed to Russia once the Kremlin was made aware of their cyber-activities and subsequently failed to condemn their acts or take reasonable action to prevent those acts.

To reiterate, the wrongful act for which the state is responsible for, is not the cyberattack that was launched by the private individual, but its failure to prevent such attacks from transpiring

296 Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 3.

297 At 3. See Dapo Akende "Oxford Statement on International Law Protections against Foreign Electoral Interference through Digital Means" (28 October 2020) Just Security <www.justsecurity.org>.

298 Shakarian, above n 278, at 64.

299 At 67.

300 At 67.

301 Oona A Hathaway "The Drawback and Dangers of Active Defense" (2014) ICCC 39 at 46.

within its own territory.[302] For example, once the Kremlin was made aware of the website, Russia had an obligation to condemn the actions of the patriotic hackers and shut down the websites that helped instigate the cyberattacks against Georgia.[303] Russia breached its obligation to "not knowingly allow their territory to be used for internationally wrongful acts using ICTs".[304] In this scenario, Georgia as the victim state, had the right to implement countermeasures against Russia or ask for those individuals to be extradited.[305]

Moreover, if pro-Russian hackers launched a cyberattack targeting Georgia's digital military systems, thus causing widespread physical destruction, then Georgia may have a right to self-defence against Russia if Russia was "unwilling to suppress" those activities.[306] Russia is not to provide malicious cyber-actors with a safe haven to conduct those attacks. This standard of attribution was established when the Taliban declined to extradite the Al-Qaeda operatives responsible for the 9/11 Terror Attack.[307] Resolution 1368 states "that those responsible for aiding, supporting or harbouring the perpetrators, organizers and sponsors of these acts will be held accountable".[308] Therefore, lethal cyber-activities conducted by patriotic hackers within the state's territory can be attributed to that state if it aided those actions.

Finally, since cyberspace is easily accessible to individuals, it will be difficult to regulate the online behaviour of citizens. It is for this reason that I uphold a high threshold of attribution. In *Nicaragua*, the ICJ held that a state can only be responsible for the actions of a non-state actor if it has "effective control" over that non-state actor.[309] The state must have near control over the non-state actor. Funding, arming and equipping a rebel group alone would not suffice.

---

302 Roscini, above n 28, at 40.

303 At 39.

304 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, above n 1, at 8.

305 Tsagourias, above n 187, at 242.

306 At 242.

307 At 242.

308 Resolution 1368 (2001) S/RES/1368 (2001).

309 *Military and Paramilitary Activities*, above n 218, at 105-115. Contrast *Prosecutor v Tadić (Judgment)* ICTY Appeals Chamber IT-94-1-A, 15 July 1999 at 131 and 145 which established a lesser standard of attribution. The state must have "overall control" over the individual or group of individuals. But note *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)* [2007] ICJ Rep 43 [Genocide] at [399]-[401] affirmed the *Nicaragua* test for attribution.

They must be involved in the group's development, tactics and strategy.[310] The non-state actor acts on the instructions and directions of that state.[311]

B Standard of Attribution

International law has not established a standard of evidence required by a state. In its drafting, the ARSIWA commentators explained that "questions of evidence and proof of such a breach fall entirely outside the scope of the articles".[312] Nonetheless, the law requires that the victim state provide factual evidence to support the allegations being made against the perpetuating state, and that the burden to prove those allegations rests on the victim state.[313] The 2015 UNGGE Report confirmed this and explicitly stated that in the context of cyberspace, accusations must be “substantiated".[314]

International courts have failed to set out a clearly defined standard of proof, stating that the standard of proof will be determined on a case-by-case basis.[315] *Nicaragua* was a case concerning the violation of force under Article 2(4) UN Charter. In that case, the ICJ explained that "clear and convincing" evidence was needed to invoke the doctrine of self-defence under Article 51 UN Charter.[316] The standard outlined by the ICJ, requires the victim state to demonstrate that "it is substantially more likely than not, that the factual claims that have been made are true".[317] The Court also noted that the standard of evidence required will depend on the severity of the violation and the unlawful act.[318] In cases concerning genocide or torture, the evidence must be definitive and "fully conclusive".[319] Violations of lesser gravity will require "convincing" evidence.[320]

---

310 Collin Allan "Attribution Issues in Cyberspace" 13 (2013) CKJICL 55 at 71.

311 At 67.

312 Draft Articles, above n 276, at 54.

313 *Oil Platforms*, above n 349, at 189.

314 Nicholas Tsagourias and Michael Farrell "Cyber Attribution: Technical and Legal Approaches and Challenges" (2020) 31 EJIL 941 at 956.

315 Aravindakshan, above n 4, at 290.

316 *Military and Paramilitary Activities*, above n 218, at 24.

317 Kristen Eichensehr "The Law and Politics of Cyberattack Attribution" (2020) 67 UCLA L Rev. 558 at 561.

318 At 561.

319 *Genocide*, above n 309, at 209.

320 Aravindakshan, above n 4, at 291.

Experts involved in the Tallinn Manual supported the ICJ's standard of attribution.[321] The Experts also suggested that a cyberattack which can be traced back to the cyber-infrastructure of a particular nation, may support a presumption of association.[322] However, indicating state responsibility based on the origins of the attack is particularly concerning as the internet is an open infrastructure and the systems used in initiating cyber-operations do not necessarily belong to attackers.[323] For example, the 2007 Estonian DDoS cyberattacks were launched from several computers located in 178 different countries.[324] The attackers relied on computer systems located within different territories and different jurisdictions. Thus, the Manual's proposal to presume association in cyberspace is dangerous because it can lead to incorrect identification and misattribution.

States cannot solely rely on the technical aspect of attribution because attribution in cyberspace is a multifaceted process, involving political, technical and legal aspects.[325] As the UNGGE report notes:[326]

> In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

For example, the United States National Security Agency developed the cyber-weapon EternalBlue which was then leaked and used by North Korea to launch the WannaCry ransomware.[327] If experts exclusively focused on the digital forensics of WannaCry, it would have led them to make a false identification. However, the ransomware note, which demanded victims pay a sum of money or risk losing their files completely, was carefully analysed by linguistic experts.[328] They found that the instructions detailed in the note were written by a non-native English speaker and dismissed the idea of United States liability.[329]

---

321 Tallinn Manual 2.0, above n 183, at 82.

322 Tallinn Manual, above n 13, at 39.

323 Clara Assumpção "The Problem of Cyber Attribution Between States" (06 May 2020) E-International Relations <www.e-ir.info>.

324 Tsagourias, above n 187, at 233.

325 Tsagourias and Farrell, above n 314, at 945.

326 *Developments in the field of information and telecommunications in the context of international security* GA Res 73/27, A/Res/60/1 (2018).

327 Delerue, above n 91, at 166.

328 Minda Zetlin "Whoever Created the WannaCry Ransomware, Analysis Shows They Speak Chinese" (29 May 2017) INC <www.inc.com>.

329 Zetlin, above n 336.

Accordingly, circumstantial evidence may be a sufficient standard of evidence for attributing low-intensity cyber-operations to a responsible state.[330] International law has accepted circumstantial evidence as an appropriate standard of evidence.[331] In *Corfu Channel*, the court acknowledged the difficulties of obtaining evidence that was under the control of another state and noted that circumstantial evidence may be appropriate in certain circumstances.[332] The ICJ added that the "proof may be drawn from inferences of fact provided they leave no room for reasonable doubt".[333] The Court permits the use of circumstantial evidence where:[334]

- The relevant direct evidence is within the exclusive territorial control of the state; and
- The circumstantial evidence furnished is consistent with or does not contradict any direct evidence produced.

The judgment in *Corfu Channel* is particularly useful in cyberspace because cyberattacks can be launched from different cyber-infrastructures that do not necessarily belong to the hostile actor. Additionally, to identify the origin of the attack, the victim state would require the full cooperation of states. However, some states may be unwilling to hand over such information, making it difficult for the victim state to pursue legal redress.

The ICJ in *Nicaragua* did not completely rule out the use of circumstantial evidence, but noted that circumstantial evidence must be read and supported by primary evidence.[335] Therefore, it can be inferred that circumstantial evidence may be an acceptable standard of evidence to prove attribution of malicious cyberattacks.

Some scholars are of the view that the standard of proof should remain high in order to uphold the credibility of cyber attribution.[336] Since attribution in cyberspace raises political and technical challenges, imposing a lower threshold of proof may lead to false accusations and

330 Tsagourias and Farrell, above n 314, at 966.
331 At 292.
332 *Corfu Channel*, above n 292, at 18.
333 At 18.
334 Aravindakshan, above n 4, at 294.
335 *Military and Paramilitary Activities*, above n 218, at 74.
336 Tsagourias and Farrell, above n 314, at 958. See Eichensehr, above n 317, at 577; and Marco Roscini "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations" (30 June 2014) 50 Texas Intl LJ 233 at 251.

increase tension among states.[337] Advocates maintain that some states are not technologically advanced and lack the resources required to disprove claims made against them.[338] Therefore, the standard should not be lowered in cyberspace because it may compromise the reliability of evidence and lead to wrongful attribution.[339]

There is merit to this argument because the standard of circumstantial evidence can be abused by the victim state and the perpetuating state. For instance, a state may falsely attribute a cyberattack to an innocent state to appear competent on the international and domestic stage or to harm the reputation of another state.[340] It is for this reason that I limit circumstantial evidence to low intensity cyber-operations.[341]

Furthermore, the ICJ made it clear that the standard of proof in international law does not demand complete confidence or absolute certainty.[342] No evidence beyond doubt is necessary under international law.[343] The high evidentiary standard outlined in *Nicaragua,* may frustrate attribution mechanisms in cyberspace.[344] Indeed, states are never going to have clear and direct evidence in this area because the technical characteristics of cyberspace means that the attacker's identity can never be 100 per cent certain.[345] This standard will enhance cyber-stability efforts and ensure that states are held legally accountable for their cyber-activities.

To summarise, this part demonstrated the challenges of attributing cyber-conduct to a state actor and examined whether the wrongful actions of a private individual can be attributed to a state.

VI Self-defence in Cyberspace

337 Aravindakshan, above n 4, at 292.

338 Milton Mueller and others “Cyber Attribution: Can a New Institution Achieve Transnational Credibility” (2019) CDR 107 at 110 at 110.

339 Eric Mejia "Act and Actor Attribution in Cyberspace A Proposed Analytical Framework" (2014) 8 SSQ 114 at 115.

340 Herbert Lin "Attribution of Malicious Cyber Incidents From Soup to Nuts" (2016) NSTL 1 at 29.

341 Aravindakshan, above n 4, at 286.

342 Tsagourias and Farrell, above n 314, at 966.

343 Roscini, above n 336, at 252. See generally Anna Riddell and Brendan Plant Evidence before the International Court of Justice (British Institute of International and Comparative Law, London, 2009) at 136.

344 Tsagourias and Farrell, above n 314, at 966.

345 Lin, above n 340, at 29.

In this chapter, I will focus on the doctrine of self-defence and outline the limitations of applying the elements of necessity, immediacy and proportionality in cyberspace.

A The Doctrine of Self-defence

Article 51 UN Charter provides an exception to the prohibition of force. It states:[346]

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Article 51 was drafted to be both objective and narrow in scope.[347] States can only use defensive force in self-defence, if they have been subject to an armed attack.[348] The ICJ in *Oil Platforms* held that the burden of proof falls on the victim state to show that an armed attack has occurred.[349]

What constitutes an "armed attack" is not defined by the UN Charter and remains subject to interpretation.[350] In *Nicaragua,* the ICJ established that not all use of force will amount to an armed attack.[351] The ICJ tried to distinguish between the "most grave use of force" from other "less grave use of force".[352] Accordingly, an "armed attack" is one which causes significant physical destruction, death or injury.[353] The "armed attack" threshold is higher than the threshold of force.[354] This distinction must be emphasised because under Article 51, actions that fall below the threshold of an "armed attack" will require a different response.[355]

---

346 Charter of the United Nations, art 51.

347 O'Connell, above n 149, at 154.

348 D.W Bowett *Self-Defence in International Law* (Manchester University Press, Manchester, 1958) at 187.

349 *Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [2003] ICJ Rep 161 at 189.

350 Abdulqawi A Yusuf, "The Notion of Armed Attack in the Nicaragua Judgment and Its Influence on Subsequent Case Law" (2012) 25 LJIL 461 at 462.

351 Ruys, above n 2, at 165.

352 *Military and Paramilitary Activities*, above n 218, at 101.

353 Weissbrodt, above n 121, at 364.

354 Yusuf, above n 350, at 463.

355 Weissbrodt, above n 121, at 362.

Interestingly, the United States does not differentiate between illegal use of force and armed attack.[356] The United States maintains that there is no threshold and the right to self-defence applies to "any illegal use of force".[357] However, this is not the dominant view among scholars who confirm the distinction made in *Nicaragua*.[358] The Tallinn Manual also firmly disagrees with this notion and holds that such an interpretation is inconsistent with the judgment in *Nicaragua*.[359] Scholars recognise the dangers of widening the scope of self-defence to include small-scale attacks as armed attacks.[360] Permitting the use of defensive force against a small-scale attack, could lead to further tension between states and risk escalation of military action.[361]

While states are growing increasingly frustrated by low-intensity cyber-operations that disrupt and degrade computer networks, none have publicly declared themselves a victim of an "armed attack" in cyberspace.[362] Most States have not accepted that low-intensity cyber-operations can amount to an "armed attack" under international law.[363] Iran, New Zealand and Germany, have all endorsed the findings in *Nicaragua* and find that the inherent right of self-defence will be held for cyber-operations that meet the threshold of an armed attack.[364]

---

356 Ryan Goodman "Cyber Operations and the U.S. Definition of "Armed Attack"" (08 March 2018) Just Security <www.justsecurity.org>.

357 Harold Koh, Legal Adviser of the United States Department of State "International Law in Cyberspace" (USCYBERCOM Inter-Agency Legal Conference on the Roles of Cyber in National Defense, Fort Meade, Maryland, 18 September 2012.

358 Brownlie, above n 89, at 272-280. See also Georg Nolte and Albrecht Randelzhofer "Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51" in Bruno Simma, and others (ed) *The Charter of the United Nations (3rd Edition): A Commentary, Volume II* (Oxford University Press, Oxford, 2012) at 1400; and Olivier Corten "A Plea Against the Abusive Invocation of Self-Defence as a Response to Terrorism" EJIL:Talk! <www.ejiltalk.org> at 1.

359 Michael Schmitt "The Use of Cyber Force and International Law" in Marc Weller (ed) *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, Oxford, 2016) 1120 at 1119.

360 Randelzhofer, above 358, at 1401. See Corten, above n 358, at 1; and Flavio Paioletti "The 21st Century Challenges to Article 51" (30 June 2021) E-International Relations <www.e-ir.info>.

361 David Kretzmer "The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum" (2013) 24 EJIL 235 at 267.

362 Hayward, above n 113, at 411.

363 Michael Schmitt "New Zealand Pushes the Dialogue on International Cyber Law Forward" (08 December 2020) Just Security <https://www.justsecurity.org>. See also "General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat", above n 109; The Federal Government of Germany, above n 109, at 15.

364 Schmitt, above n 363; "General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat", above n 109; and Federal Government of Germany, above n 109, at 15.

However, cyberspace impacts every aspect of our modern lives and our reliance on it means that we must examine whether small-scale effects may eventually amount to an armed attack. The ICJ in *Nicaragua* did not deny that a series of small-scale attacks may "collectively" satisfy the threshold of an armed attack.[365] The "pinprick" theory maintains that multiple small-scale attacks can together satisfy the threshold of an "armed attack" under Article 51 UN Charter.[366] The attacks on their own may not satisfy the threshold but cumulatively, they would.[367] Thus, the gap between "use of force" and an "armed attack" may be narrowed in limited circumstances.

The theory has gained support among the international community.[368] Indeed, states have previously responded to a series of small-scale incursions.[369] For example, the United States in *Oil Platforms* argued that it was responding to a number of attacks committed by Iran, including the attack on the *Sea of Isle City* and *Samuel B. Roberts*.[370] While the Court dismissed the claim of self-defence, the majority agreed that low-levels of violence, when accumulated, may satisfy the threshold of an armed attack.[371] This was affirmed in *Armed Activities,* where a series of acts can amount to an armed attack, that would not otherwise have, had it occurred in isolation.[372] As a result, it could be asserted that a series of related malicious cyber-operations committed by the same state actor, may amount to an armed attack under Article 51 UN Charter.

It should be noted that accumulative operations must rise to the threshold of force under Article 2(4) UN Charter.[373] For example, a malicious cyber-operation that temporarily disrupts the power grid of a small neighbourhood could amount to an armed attack in accumulation. In isolation, the cyberattack may not be viewed as sufficiently grave to satisfy the threshold of an

365 *Military and Paramilitary Activities*, above n 218, at 165.

366 At 165.

367 At 165.

368 Monica Hakimi and Jacob Katz Cogan "The Two Codes on the Use of Force" (2016) 27 EJIL 257 at 272.

369 Christine Gray *International Law and the Use of Force* (3rd ed, Oxford University Press, New York, 2008) at 155.

370 *Oil Platforms*, above n 349, at 191.

371 At 191.

372 *Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda) (Judgment)* [2005] ICJ Rep 168 [Armed Activities] at 223.

373 Yoram Dinstein *War Aggression and Self-Defence* (6th ed, Cambridge University Press, Cambridge, 2016) at 275.

armed attack. However, as previously noted, cyber-operations rarely result in physical effects. Thus, the pinprick theory may continue to exclude low-intensity cyber-operations that aim to disrupt and undermine the economic and political infrastructures of a nation.

Finally, the ICJ concludes that "a mere frontier incident" does not amount to an armed attack.[374] This view found support in the Eritrea-Ethiopia Claims Commission which affirmed that "localised border encounters between small infantry units, even those involving the loss of life, do not constitute an armed attack for purposes of the Charter".[375] However, this judgment has been met with criticism. Scholars, notably, Dinstein and Hargrove, question the distinction outlined in *Nicaragua* claiming that it narrows the scope of self-defence and allows for lower levels of violence.[376] They find that such a distinction may encourage low-intensity military action because it takes away the victim state's right to self-defence [377]

B Necessity, Proportionality and Immediacy

The inherent right of self-defence under customary international law is subject to the elements of necessity, proportionality and immediacy.[378] The most important elements of these are necessity and proportionality. As highlighted during the Falklands War, the geographical distance between Britain and the Falklands meant that it would take significant time for Britain to reach the Falklands port.[379] The temporal remoteness of Britain's use of defensive force was justified within the grounds of self-defence.[380] Its remedial action to abate the attacks of the occupying forces was necessary.[381] The criterion of proportionality and immediacy must always be read in light of necessity.[382]

1 Necessity

---

374 *Military and Paramilitary Activities*, above n 218, at 103-104.

375 *Eritrea Ethiopia Claims Commission, Partial Award, Jus ad Bellum, Ethiopia's Claims* 1–8, The Hague, [2005].

376 John Hargrove "The Nicaragua Judgment and the Future of the Law of Force and Self-defense" (1987) 81 AJIL 135 at 139. See also Dinstein, above n 373, at 195.

377 Gray, above n 369, at 179-180. See also Hargrove, above n 376, at 139; Dinstein, above n 373, at 195.

378 *Military and Paramilitary Activities*, above n 218, at 103; and *Oil Platforms*, above n 349, at 196. See Buchan, above n 90, at 364.

379 Kinga Tibori Szabó *Anticipatory Action in Self-Defence* (T. M. C. Asser Press, The Hague, 2011) at 155.

380 At 154-155.

381 SC Res 502, S/Res/502 (1982).

382 Oscar Schachter "The Right of States to Use Armed Force" (1984) 82 MLR 1620 at 1637.

The doctrine of necessity maintains that the victim state had no other reasonably peaceful measures open to them and that defensive force was of "last resort".[383] The concept of necessity may take a different dimension in cyberspace. Before responding to an attack, the victim state must ensure that the cyberattack was purposeful and intended, and examine whether "less intrusive means" may be adopted.[384] The state can only use defensive force in self-defence if the purpose of maintaining its security cannot be achieved through diplomatic means, countermeasures or other cyber-defences.[385] For example, if the cyberattack can be halted by blocking access to a particular network, then defensive force will not be a reasonable option.[386] Indeed, if the victim state has mechanisms set up to prevent a cyberattack from materialising, then self-defence may not be necessary. This calculation of necessity may impose a positive obligation on states to strengthen their "passive or active cyber-defences".[387] However as the UNGGE correctly argues, some states do not have the adequate resources to build their cyber-defences.[388]

Furthermore, the victim state must only do what is necessary to repel the armed attack.[389] In *Oil Platforms*, the ICJ claimed that the measures adopted by the United States did not meet the element of necessity.[390] It argued that the United States decision to attack Iran's oil platforms was not necessary to repel the attack that targeted its merchant vessel and military vessel.[391] Thus, a targeted action is expected to abate the armed attack or further armed attacks to support the objectives of the self-defence doctrine.[392]

In cyberspace, it can be difficult to detect an attack and the identity of the attacker. Suppose the victim state only detects the cyberattack after it has been completed. In that case, the victim state may be expected to take action outside of self-defence if there are no additional risks of a

---

383 James Green *The International Court of Justice and Self-Defence in International Law* (Hart Publishing Ltd, Portland, 2009) at 78.

384 Roscini, above n 277, at 119.

385 Delerue, above n 91, at 480.

386 At 480.

387 Carlo Focarelli "Self-defence in Cyberspace" in Nicholas Tsagourias and Russell Buchan (eds) Research Handbook on International Law and Cyberspace (Edward Elgar Publishing, Cheltenham, 2015) 255 at 273.

388 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, above n 1, at 2.

389 *Oil Platforms*, above n 349, at 198.

390 At 198.

391 At 196 – 198.

392 At 199.

future attack.[393] In order to abate the attack, forcible action should be taken against the computer network which developed or launched the cyber-operation.[394] The victim state must verify the identity of the hostile cyber-actor to determine whether extradition may be a more appropriate measure. However, the victim state may not be able to determine the accurate cyber-network used to conduct the cyberattack because the attackers can disguise or hide the origins of the operation.[395] The operation may be conducted and launched by the cyber-infrastructure of an innocent third party, making it illegal to take forcible action under Article 51, unless the third party condones the attack or does not do enough to prevent the attack.[396]

2 Immediacy

The element of immediacy requires that the victim state respond within a timely manner that is necessary to repel the attack.[397] It provides a limit on the use of force and ensures that the defensive action is not to punish the attacker but to prevent the armed attack.[398] Since cyber-operations are launched anonymously, the victim state will have to delay its response until it can uncover the attacker's identity.[399] As Dinstein accurately points out, some circumstances may justify a long lapse of time between the initial attack and the response to the attack.[400] He adds that merely waiting a longer period of time to respond does not mean that the response is retaliatory or punitive.[401] In cyberspace, it may be necessary to delay defensive action because it can be difficult to determine who is responsible for the cyberattack. Thus, a more flexible interpretation of immediacy will be required in cyberspace.[402]

The degree of immediacy remains debated in international law. It is unclear whether a state can act in self-defence to abate an ongoing armed attack, or whether a state can use defensive force to deter future armed attacks, or whether it can use defensive force once the armed attack has been completed.[403] If we take a purely textual interpretation of Article 51, self-defence will

393 Delerue, above n 91, at 480.
394 At 479 – 480.
395 Tsagourias, above n 187, at 233.
396 Green, above n 383, at 101.
397 At 102.
398 Roscini, above n 277, at 120.
399 Lin, above n 340, at 41.
400 Dinstein, above n 373, at 252.
401 At 252.
402 Roscini, above n 277, at 120.
403 Ruys, above n 78, at 8.

only be triggered once an armed attack has occurred.[404] However, Article 31 of the 1969 Vienna Convention on the Law of Treaties explains that interpretation of articles must not be "manifestly absurd or unreasonable".[405] It is difficult to completely dismiss the notion of anticipatory self-defence and demand that states fall victim to an armed attack before taking defensive action.[406]

The *Caroline* doctrine of anticipatory self-defence allows the victim state to use preemptive force when it is faced with an "imminent" armed attack.[407] The doctrine applies when the "necessity of self-defence is instant, overwhelming, leaving no choice of means, and no moment for deliberation".[408] The ICJ in *Nicaragua* did not clarify the issue of anticipatory self-defence.[409] In the aftermath of the 2001 Terror Attack, President George W Bush stated that states must "confront the worst threats before they emerge".[410] The Bush Doctrine expanded the scope of anticipatory self-defence to include pre-emptive or preventive strikes against emerging threats.[411] Nonetheless, the ICJ in *Armed Activities* did not uphold the Bush Doctrine. It found that Uganda's use of self-defence was unlawful because Article 51 "does not allow the use of force by a State to protect perceived security interests".[412] The ICJ explained that Uganda's actions were not in response to an actual attack.[413]

The Tallinn Manual endorses the imminence criterion established in *Caroline* and maintains that imminence is satisfied when "an adversary state is clearly committed to launching an armed attack and the victim state will lose its opportunity to effectively defend itself unless it

404 At 9-10.

405 Vienna Convention on the Law of Treaties, art 31.

406 Oscar Schachter "In Defense of International Rules on the Use of Force" (1986) 53 Chicago Law Review 113 at 136.

407 Judith Gardam *Necessity, Proportionality and the Use of Force by States* (Cambridge University Press, Cambridge, 2004) at 146.

408 Letter from Daniel Webster (United States Secretary of State) to Lord Ashburton regarding the *Caroline* case (6 August 1842).

409 *Military and Paramilitary Activities*, above n 218, at 103.

410 George W Bush, President of the United States "Pre-emptive military action" (West Point Military Academy graduation, New York, 01 June 2002).

411 President of the United State, George W Bush "The National Security Strategy of the United States of America" (September 2002) The White House <https://georgewbush-whitehouse.archives.gov> at 15.

412 *Armed Activities*, above n 372, at 223.

413 At 222.

acts".[414] The experts concluded that "the last possible window of opportunity" allows states to use defensive force in anticipation of an attack.[415]

The criteria set out in *Caroline* may help address the threats posed in cyberspace.[416] In light of this, it is important to examine at which stage anticipatory self-defence may be permitted in cyberspace. Specifically, how imminent must the cyberattack be before the victim state can take defensive action under Article 51 UN Charter?[417] Nicholas Tsagourias and Michael Farrell reflected on the existing cyber-framework established by the United States Director of National Intelligence.[418] They noted that a malicious cyber operation can be broken down into six stages:[419]

1. Preparatory stage of target identification;
2. Reconnaissance and weaponization;
3. Engagement and presence stage of delivery;
4. Exploitation;
5. Installation and actions on objective; and
6. Effects and consequences stage.

The first stage, the preparatory stage of target identification, is concerned with information gathering and determining the intended target of attack.[420] At this stage, it is difficult to anticipate an attack because the cyber-weapon has not been developed.[421] The second stage, reconnaissance and weaponisation, is the development of the malicious code used to carry out the strategic objectives of the hostile cyber-actor.[422] At this point, the cyber-actor has not launched the cyberattack and they may choose not to carry out the attack. The intention of the attacker is still unknown. Taking anticipatory action at this stage may escalate tension and disrupt international security.

---

414 Geoffrey DeWeese "Anticipatory and Pre-emptive Self-Defense in Cyberspace: The Challenge of Imminence" AOC (2015) 81 at 87.

415 Hayward, above n 113, at 415.

416 Focarelli, above n 387, at 273.

417 It should be noted that not all cyberattacks come in this shape or form and that this is one model of a cyberattack. See Tsagourias and Farrell, above n 314, at 947 "there is no standardized model of cyber attack".

418 At 947. See also Office of the Director of National Intelligence "Building Blocks of Cyber Intelligence" ODNI <www.dni.gov>.

419 At 947.

420 Office of the Director of National Intelligence, above n 418.

421 Office of the Director of National Intelligence, above n 418.

422 Office of the Director of National Intelligence, above n 418.

During the engagement and presence stage of delivery, the cyber-actor has delivered the malicious code to the intended target.[423] This could potentially trigger a right to anticipatory self-defence. However, at this stage, the cyber-actor has the opportunity to disable the code. Additionally, the cyber-capabilities of the victim state may be able to thwart the cyber-threat.

In the fourth stage, the cyber-operation has successfully exploited the cyber-vulnerabilities of the target state.[424] At this stage, the right to anticipatory self-defence is more likely as the state has expressed its clear intention to attack. Yet, the full effects of the operation may be unknown and the cyberattack may not rise to the level of an armed attack. In the fifth stage, installation and actions on objective, the cyber-weapon has established control over the computer networks of the target state.[425] Anticipatory self-defence is permitted. The effects and consequences stage of the operation is the final stage of a cyberattack.[426] The cyberattack has been sufficiently completed and anticipatory self-defence is no longer required.

As demonstrated, the technological characteristics of how cyber-operations are designed and used make it difficult to determine the exact timing of a cyberattack. Cyber-operations can take months or even years to develop, and can be launched within nano-seconds, making it hard to foresee a cyberattack.[427] They are often prepared in secrecy and may only be detected long after the initial attack.[428] For example, it is alleged that the United States with the support of Israel, began developing the Stuxnet malware in 2006.[429] However, the software was only discovered in 2010, years after it was developed and launched.[430] Consequently, it is difficult to ascertain the imminent nature of a cyberattack because of the degree of knowledge required.

Schmitt notes three factors to consider when taking defensive action in response to a prospective cyberattack:[431]

---

423 Office of the Director of National Intelligence, above n 418.

424 Office of the Director of National Intelligence, above n 418.

425 Office of the Director of National Intelligence, above n 418.

426 Office of the Director of National Intelligence, above n 418.

427 Office of the Director of National Intelligence, above n 418.

428 Dieter Fleck "Searching for International Rules Applicable to Cyber Warfare – A critical First Assessment of the New Tallinn Manual" (2013) 18 JCSL 331 at 334.

429 Zetter, above n 119, at 194.

430 At 237.

431 Michael Schmitt *Essays on Law and War at the Fault* (TMC Asser Press Springer, The Hague, 2012) at 41.

> (a) The CNA [Computer Network Attack] is part of an overall operation culminating in armed attack;
>
> (b) The CNA [Computer Network Attack] is an irrevocable step in an imminent (near term) and probably unavoidable attack; and
>
> (c) The defender is reacting in advance of the attack itself during the last window of opportunity available to effectively counter the attack.

Schmitt's analysis recognises that cyber-operations can be launched within nano-seconds, causing potentially destructive effects. He notes that the decision to use force in anticipatory self-defence should be judged within a reasonable timeframe on a case-by-case basis. Nonetheless, Schmitt's determinations are "purely speculative" because most cyber-operations are conducted in secret, making it difficult to trace.[432]

3 Proportionality

Proportionality is an important aspect of self-defence in customary international law. Some commentators have argued that proportionality refers to the "scale and effects" of the original attack.[433] The force used to counter the attack must be reasonably equal to the original attack.[434] However, according to James Green, proportionality under international law is concerned with the measures required to defend against the initial attack.[435] States have previously used defensive force that may appear disproportionate when considering the scale and means of the initial attack, but were sufficiently necessary to repel or deter the initial attack.[436] For example, during the Gulf Conflict 1991, Security Council Resolution 678 authorised UN Members to take "all necessary means" to remove Iraqi forces and liberate the people of Kuwait.[437] Once the threat was alleviated and Iraqi forces had been removed, any forcible response after that would have gone beyond the requirement of proportionality under Article 51.[438] Thus, the

---

432 Focarelli, above n 387, at 273.

433 Sina Etezazian "The nature of the self-defence proportionality requirement" (2016) 3 JUFIL 260 at 265. See Green, above n 383, at 88.

434 At 265.

435 Green, above n 383, at 88.

436 At 89.

437 SC Res 678, S/Res/678 (1990).

438 Green, above n 383, at 90.

proportionality criterion is not concerned with the "scale and means of the attack", it is concerned with what is necessary to achieve the state's defensive purpose.[439]

In cyberspace, it is difficult to evaluate the proportionate responses required to alleviate a cyberattack because of its direct and indirect impact.[440] Cyber-operations can have "bleed-over" effects, resulting in unintended consequences that only appear later.[441] For example, in 2012, Saudi Arabia's state-owned oil facility, Saudi Aramco, was subject to a cyberattack. Operation Shamoon was a virus that wiped data and destroyed 30,000 computers.[442] Saudi Arabian computer forensic experts took two weeks to assess the full damage, in contrast to traditional attacks which can be assessed within hours.[443] Saudi Arabia, which is the world's largest supplier of oil, claimed that the attack did not have a significant impact on its production.[444] A thorough damage report was required to ensure that the cyberattack did not result in significant economic or physical damage. Indeed, it is necessary to carefully assess the damage of the cyberattack because quick determinations can lead to disproportionate responses.[445]

In addition, the harmful cyber-effects felt in one country may be less devastating in another country. This raises the question of how proportionality will be measured. As previously mentioned, some states have not sufficiently built their cyber-defences to combat incoming cyberattacks. It is unclear whether proportionality should be measured against the cyber-capabilities of the hostile state. Thus, the interpretative nature of an effects-based approach can make it difficult to calculate a legally proportionate response in cyberspace.[446]

Furthermore, the proportionality of the response is not dictated by the instrument used to launch the attack.[447] A cyberattack does not require a cyber-response in self-defence. Scholars argue

---

439 At 89.

440 Mejia, above n 339, at 116.

441 Schmitt, above n 359, at 1125.

442 Lily Newman "The Iran Hacks Cybersecurity Experts Feared May Be Here" (18 December 2018) Wired <www.wired.com>.

443 Tobias Feakin "Developing a Proportionate Response to a Cyber Incident" (August 2015) Council of Foreign Policy <https://cdn.cfr.org> at 2.

444 Sahar Alshathry "Cyber Attack on Saudi Aramco" (2017) 11 IJMIT 3307 at 3037.

445 Feakin, above n 443, at 3.

446 Matthew Waxman "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions" (2013) 89 Intl L Stud 109 at 112.

447 Tallinn Manual, above n 13, at 62.

that conventional weapons may be used as a proportionate response to a cyberattack.[448] This is important to note because a hostile state may not have a "sufficiently developed computer network" to target.[449] For example, North Korea is a major aggressor in cyberspace, often launching large-scale cyber-theft campaigns.[450] However, if North Korea launched a cyberattack, manipulating air traffic controls resulting in a plane crash, the victim state would have little redress in the way of cyberspace. North Korea's critical infrastructure is not dependent on information technology.[451] It is isolated and restricted from the digital domain, making it less vulnerable to retaliatory cyberattacks.[452] Thus, a non-kinetic cyber-response may not always be an adequate response to a cyberattack.

A proportionate kinetic attack may be necessary in some circumstances. For example, the secret nature of cyber-operations and their sophisticated features can make it difficult for a victim state to determine the vulnerability that the cyber-operation is exploiting. The victim state may not be able to abate the attack through cyber-means and has no option but to launch a traditional attack against the routers responsible for the cyber-operation. This could also include striking the cyber-infrastructures that are responsible for the cyberattack in order to disable it.

States have also tried to determine whether a kinetic attack in response to a cyberattack can be proportionate. United States National Security Agency Chief, Michael Rogers, concludes that "because an opponent comes at us in the cyber-domain doesn't mean we have to respond in the cyber-domain".[453] Clarifying its position that a cyberattack does not require a cyber-response, on 14 September 2019, Houthi rebels launched a drone strike on Saudi Arabia's state-owned oil facility, Saudi Aramco.[454] Secretary of State Mike Pompeo accused Iran of being involved

448 Jarno Limnéll "Proportional Response to Cyberattacks" (2017) 1 CIS 37 at 47; Focarelli, above n 387, at 274; Roscini above n 28, at 90; Fenkin above n 443, at 3.

449 Roscini, above n 277, at 120.

450 Morten Larsen "While North Korean Missiles Sit in Storage, Their Hackers Go Rampant" (15 March 2021) Foreign Policy <https://foreignpolicy.com>.

451 "North Korea's Offensive Cyber Program Might Be Good, But Is it Effective?" (25 October 2017) Council on Foreign Relations <www.cfr.org>.

452 Saira Asher "What the North Korean internet really looks like" (21 September 2016) BBC News <www.bbc.com>.

453 Joe Gould "US Cyber Commander: Hackers Will 'Pay a Price'" (11 May 2015) Defense News <www.defensenews.com>.

454 Ben Hubbard and others "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran" (14 September 2019) New York Times <www.nytimes.com>.

and discussed launching a cyberattack in response.[455] This suggests that cyber-weapons are not limited to cyber-conflict.

Furthermore, Germany, Finland, New Zealand and France, all maintain that a conventional kinetic response may be an appropriate proportionate response to a cyberattack.[456] In March of 2021, the United Kingdom updated its cyber-strategy policy and included non-kinetic counter operations in response to cyberattacks. They emphasised that they may even launch a nuclear attack in response to a grave cyber-operation.[457] Other states that have released national statements concerning the applicability of international law in cyberspace, namely, Iran, Estonia and the Czech Republic, do not expressly condemn the use of non-kinetic weapons in response to a cyberattack.[458] Instead, they remain silent on the matter.

Nonetheless, it is a commonly held view that adopting a kinetic response may increase the risk of escalation and should, therefore, be limited to cases of exceptional gravity.[459] States who choose to launch a kinetic response should only do so when the degree of attributional certainty is high and the cyber-operation has reached the threshold of an armed attack.[460] Indeed, if the cyberattack leads to loss of life or severe physical destruction, then kinetic measures may be employed. Limiting retaliatory responses to those operations will encourage states to consider a range of responses, including economic and diplomatic measures.

---

455 David E Sanger and Julian Barnes "The Urgent Search for a Cyber Silver Bullet Against Iran" (23 September 2019) New York Time <www.nytimes.com>.

456 Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 3. See also Ministry of Foreign Affairs Finland, above n 109, at 6; Federal Government of Germany, above n 109, at 15; Ministry of Armed Forces (France), above n 192, at 8.

457 Cabinet Office (United Kingdom) "Policy Paper: Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy" (16 March 2021) GOV.UK <www.gov.uk>.

458 "General Staff of Iranian Armed Forces Warns of Tough Reaction to any Cyber Threat", above n 109. See also Richard Kadlčák, Ministry of Foreign Affairs and Trade for the Cyber Security Department and Special Envoy for Cyber Space, "Special Envoy for Cyberspace Director of Cybersecurity Department of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations," (United Nations, New York, 11 February 2020); Kersti Kaljulaid, President of Estonia, "President of the Republic at the opening of CyCon 2019" (CyCon in Tallinn Estonia, 29 May 2019)

459 Delerue, above n 91, at 482.

460 Feakin, above n 443, at 3.

Yet, state practice in this area of cyberspace is significantly lacking. The secret security measures of cyberspace means that states are unwilling to disclose their cyber-strategy.[461] For example, the United States has repeatedly touted that it will carry out "proportionate responses" in the face of cyberattacks, but it has not explained what those "proportionate responses" may be.[462] Victim states are usually left pondering how to respond to the unique consequences of cyber-operations. In order to establish an international norm of what may be a proportionate response in cyberspace, states must be willing to share information and report on their cyber-measures.

In the next section, I will examine Israel's use of cyber-force against Iran. Since such instances are rare in cyberspace, it must be noted that the case study below merely adds to the literature of what may be a permitted response in the cyber-domain.

C Adversaries in Cyberspace: Israel and Iran

In examining how states may respond in cyberspace, it is important to consider the behaviour of states. As Kristen Eichensehr explains:[463]

> Understanding state behavior matters because it is one of two components of customary international law, which requires (1) general and consistent state practice that is (2) undertaken out of a sense of legal obligation (opinio juris).

The 2020 cyber-conflict between Iran and Israel is a notable case study for examination.[464]

In April 2020, Iran allegedly launched a cyberattack against Israel's water treatment facilities.[465] The cyberattack attempted to shut down Israel's water supply by programming its system to add mass amounts of chlorine.[466] The operation caused minor disruptions in Israel's water system but ultimately failed to cause significant damage to its infrastructure.[467] Although,

---

461 Hubbard and others, above n 454.

462 Hubbard and others, above n 454.

463 Kristen Eichensehr "Cyberattack Attribution and International Law" (24 July 2020) Just Security <www.justsecurity.org>.

464 Lindsay Hughes "Israel vs. Iran: The Deadly Cyberattacks Continue" Future Directions International (01 July 2020) <www.futuredirections.org.au>.

465 Gil Baram and Kevjn Lim "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks" (5 June 2020) Foreign Policy <https://foreignpolicy.com>.

466 Hughes, above n 464.

467 Hughes, above n 464.

the cyberattack did not meet the "armed attack" threshold, Israel launched a cyberattack targeting Iran's computer networks.[468] This interrupted trade routes near the Strait of Hormuz and triggered road and waterway congestion for several days.[469] Israel Defense Force Chief of Staff, Aviv Kochavi confirmed the attack and stated that Israel "will continue acting [against enemies] with a mix of instruments".[470]

Iran's initial cyberattack was thwarted by Israel's cyber-capabilities and did not require any further action.[471] Israel failed to meet the element of necessity because the measures adopted were not required to achieve the objective of self-defence.[472] In addition, Iran's attack on Israel's water treatment facility was routed through various cyber-infrastructures, including the servers of the United States and Europe.[473] Israel could not conduct an attack targeting the cyber-networks of its allies, despite, the attack being launched from those networks.[474] It would have been unlawful to take forcible action against the cyber-infrastructure of an innocent third state. However, should the attack have risen to the level of an armed attack, it would be difficult to maintain that Israel could not take any forcible action because it was routed through different servers, outside of Iranian territory. This demonstrates the difficulty of applying the doctrine of necessity in cyberspace, as Israel had limited opportunities to abate the attack.

Israel launched its cyberattack two weeks after the initial attack to demonstrate its advanced cyber-capabilities and to deter any future cyber-aggressors.[475] While states can use immediate defensive force, immediacy does not require the victim state to do so. Instead, the victim state is required to respond within a reasonable time frame to ensure that UN processes, including reporting attacks to the Security Council and exercising diplomatic measures outside of defensive force, are considered. [476] Understandably, Israel may not have been able to respond immediately because of the anonymous nature of cyberspace. The anonymity of cyberspace means that Israel had to delay its response until it could correctly identify the perpetrator.

---

468 Baram and Lim, above n 465.

469 Baram and Lim, above n 465.

470 Aviv Kochavi, Major General of Israel Defense Force "Cyberwar with Iran" (Home Front Command Replacement Ceremony, Tel Aviv, 19 May 2020).

471 Baram and Lim, above n 465.

472 Joby Warrick and Ellen Nakashima "Officials: Israel linked to a disruptive cyberattack on Iranian port facility" (19 May 2020) The Washington Post <www.washingtonpost.com>.

473 Warrick and Nakashima, above n 472.

474 Delerue, above n 91, at 479.

475 Baram and Lim, above n 465.

476 Dinstein, above n 373, at 252.

Nevertheless, Israel's use of defensive force to deter future threats that have not yet materialised is questionable.[477] The *Caroline* doctrine of self-defence permits defensive force as a "last resort". Under international law, Israel would have been expected to initiate diplomatic dialogue through a third party, or to implement non-forcible countermeasures in order to cease potential cyber-operations committed by Iran in the future.[478]

Furthermore, the intensity of Israel's response went beyond the measures required to repel the attack. Israel's cyberattack created long queues, halted trade and caused "total disarray".[479] The retaliatory and punitive nature of Israel's cyberattack goes beyond the scope of self-defence.[480]

The recent cyber-conflict between Iran and Israel has not helped clarify the position of international law in cyberspace. States and the wider international community have not publically condemned Israel's cyber use of force or expressly endorsed it. From a purely political perspective, it can be assumed that states are reluctant to support forcible measures against a cyberattack that has not materialised or appears invisible.[481] States also try to avoid endorsing military action that may sever diplomatic and economic ties.[482]

Additionally, past behaviour suggests that Israel interprets international law more exceptionally. For example, in 1981, Israel launched an attack against Iraq's Osiraq nuclear facility.[483] Israel argued that it was defending itself from a threat that may arise in the future.[484] The UNSC did not accept Israel's claim of self-defence and condemned its actions as unlawful under international law.[485] Even more relevant, in April 2021, Israel launched a cyberattack against the industrial control systems of Iran's nuclear enrichment facility.[486] The attack

477 Kretzmer, above n 361, at 239.
478 At 239.
479 Hughes, above n 464.
480 Dinstein, above n 373, at 252.
481 Waxman, above n 446, at 120.
482 At 120. See generally Joseph Nye Jr. "Deterrence and Dissuasion in Cyberspace" (2017) Intl Security 44 at 59.
483 Hakimi and Cogan, above n 368, at 284.
484 At 284.
485 At 284.
486 Martin Chulov "Israel appears to confirm it carried out cyberattack on Iran nuclear facility" (11 April 2021) The Guardian <www.theguardian.com>.

disrupted the power supply of Iran's nuclear centrifuges, resulting in physical damage.[487] This attack could be viewed as a breach of international law because at the time of the attack, the nuclear reactor did not pose an actual threat of an armed attack against Israel. For these reasons, cyber-threats and cyberattacks continue to operate within a grey zone of the law.

D Collective Self-defence

Article 51 UN Charter authorises the use of collective self-defence, that is, the use of defensive force by a third state on behalf of the victim state.[488] In other words, a non-injured state may respond on behalf of the victim state and legally support the victim state's effort to exercise its right to self-defence.[489] *Nicaragua* confirmed that collective self-defence is subject to the same rules that govern the law of individual self-defence.[490] Nonetheless, it added two additional features to distinguish collective self-defence from individual self-defence.[491] First, the victim state must assert that it has been the victim of an armed attack. The third state cannot determine that by its own evaluation and volition.[492] Second, the victim state must request the support of the third state.[493] The victim state is not obligated to make this request through the UNSC, however, "the absence of a report may be one of the factors indicating whether the state in question was itself convinced that it was acting in self-defence"[494] If the third state responds to an armed attack without the consent of the victim state then that attack will be deemed unlawful.[495]

The general applicability of the UN Charter implies that collective self-defence is permitted in cyberspace. This is confirmed under Rule 16 of the Tallinn Manual.[496] Additionally, in 2011,

---

487 Chulov, above n 486.

488 Focarelli, above n 387, at 275.

489 Laura Visser "Intervention by invitation and collective self-defence: two sides of the same coin?" (2020) 7 JFIL 292 at 302.

490 *Military and Paramilitary Activities*, above n 218, at 105.

491 At 105.

492 Gray, above n 369, at 169.

493 *Military and Paramilitary Activities*, above n 218, at 105.

494 At 105.

495 Focarelli, above n 387, at 276. See James Green "The 'additional' criteria for collective self-defence: request but not declaration" (2017) 4 UFIL 4.

496 Tallinn Manual, above n 13, at 67.

the United States, Australia and New Zealand confirmed their commitment to the 1951 Security Treaty (ANZUS Treaty) and added:[497]

> … in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.

Based on the commitment of states to uphold the UN Charter in cyberspace, it can be assumed that the notion of collective self-defence applies in cyberspace.

Collective self-defence may provide solace for victim states that are not technologically advanced enough to respond to a cyberattack.[498] It may be an effective mechanism to prevent an attack by a perpetrating state on behalf of the victim state. During the 2020 UNGGE session, the Non-Aligned Movement called on states to:

> Provide to the developing countries upon their request with assistance and cooperation, including through financial resources, capacity-building and technology transfer in ICT areas while taking into account specific needs and particularities of each recipient State.

This could be in the form of collective self-defence as states who have been subject to a cyberattack may request the assistance of a third state.

In this chapter, I explained how the orthodox doctrine of self-defence can be applied in cyberspace and noted some of the challenges associated with the doctrine.

VII Responses in Cyberspace

This chapter will discuss the various measures that are open to victim states in cyberspace. The responses discussed below are limited to state-sponsored cyber-activity as this is the main focus of my paper.

---

497 Hillary Rodham Clinton, Secretary of State, Leon Panetta, Secretary of Defense, Kevin Rudd, Minister for Foreign Affairs, and Stephen Smith, Minister for Defence "U.S.-Australia Ministerial Consultations 2011 Joint Statement on Cyberspace" (26th Australia-United States Ministerial Consultations, Washington D.C., 15 September 2011).

498 Roscini, above n 277, at 120.

A Countermeasures

The law of countermeasures allows states to respond to international violations that fall below the threshold of an armed attack.[499] The 2015 UNGGE Report concluded that the law of state responsibility applies in cyberspace.[500] The Report affirmed that "states must meet their international obligations regarding internationally wrongful acts attributable to them under international law".[501] Thus, the law of countermeasures can be applied in cyberspace.

Article 49 ARSIWA, affirms that any state that has been victim of an internationally wrongful act or omission may respond by imposing countermeasures against the responsible state. Schmitt describes "countermeasures" as:[502]

> State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions.

Countermeasures are actions that would be unlawful under international law. However, they may be applied when a state has committed an internationally wrongful act and when that act can be attributed to a state.[503] The wrongful act may be a breach of a "state's treaty obligations or customary international law".[504] Such violations can include obligations relating to bilateral commitments or obligations under the principle of non-intervention.[505]

Once again, the wrongful act must be correctly attributed to the perpetrating state before engaging in countermeasures. Indeed, attribution must reach "reasonable certainty" before countermeasures can be imposed by the victim state.[506] In cyberspace, the attacker may launch a series of cyberattacks from unsuspecting computers and networks.[507] If the injured state

499 Jeff Kosseff "Collective Countermeasures in Cyberspace" (2020) 10 JICL 18 at 18.
500 Michael Schmitt ""Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law" (2014) 54 VJ Intl L 698 at 700.
501 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, above n 1, at 13.
502 Schmitt, above n 500, at 700.
503 At 703.
504 At 704.
505 At 703.
506 Draft Articles, above n 276, at 39.
507 Hathaway, above n 301, at 47.

responds by launching its own countermeasures, it must ensure that it targets and disables the computer network of the suspected attacker.[508] Countermeasures cannot target the computer networks of innocent users.

The law places strict limits on the use of countermeasures. In particular, states cannot impose countermeasures once the wrongful act has been completed. The ICJ in *Gabčíkovo-Nagymaros Project* affirmed that countermeasures are reactive and "must be taken in response to a previous international wrongful act of another State".[509] While they are reactive, countermeasures cannot be imposed as a form of punishment. As was proclaimed in the *Air Service* agreement of 1978, countermeasures "should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute".[510] The ICJ added that the "injured state must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it".[511] Thus, countermeasures can only be applied if the responsible state has no intention of ceasing its wrongful conduct or rectifying the wrongful act.[512]

The reactive nature of countermeasures can be challenging in cyberspace because cyber-operations are covert and may not be immediately detected or easily traceable.[513] For example, malware that is embedded in an email chain, may take months to effectively disrupt the computer networks of a state. The victim state may not detect the incoming operation or grasp its full effects until it has been completed.[514] However, once the attack has been completed and the aggressor state has ceased the wrongful action, the victim state may not impose countermeasures.[515] It would be unlawful because countermeasures must cease once the perpetrating state has ceased its cyberattack.[516]

If an ongoing cyberattack is detected, the victim state will request the aggressor state to cease its actions. If the responsible state refuses to do so, the victim state will notify the responsible

508 Schmitt, above n 500, at 707.

509 *Gabčíkovo-Nagymaros Project (Hungary/Slovakia) (Judgments)* [1997] ICJ Rep 7 at 52.

510 At 56.

511 At 53.

512 Schmitt, above 500, at 715.

513 Christopher Chivvis and Cynthia Dion-Schwarz "Why It's So Hard to Stop a Cyberattack — and Even Harder to Fight Back" (30 March 2017) Rand Cooperation <www.rand.org>.

514 Chivvis and Dion-Schwarz, above n 513.

515 Jeff Kosseff "Retorsion as a Response to Ongoing Malign Cyber Operations" (2020) ICCC 9 at 11.

516 Troy Anderson "Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals" (2016) 34 AJICL 136 at 148.

state of its intention to implement countermeasures. This requirement limits the state's ability to take immediate and effective action in cyberspace.[517] However, the ILC recognises that a "state may take such urgent countermeasures as are necessary to preserve its rights".[518] This grants states with an opportunity to conduct active countermeasures. The United Kingdom, the United States, the Netherlands, Israel, France, and New Zealand all support this right.[519] Countermeasures that are implemented in this way are more effective in cyberspace. Indeed, the rapid speed of cyberspace means that cyberattacks demand immediate attention and the element of notification may stall one's ability to alleviate the attack.[520]

Moreover, Article 51 of ARSIWA states that "countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question".[521] Since countermeasures are not intended to be punitive, the victim state cannot impose disproportionate measures "even if only an action of that intensity and scope would suffice to convince the responsible State to desist in its intentionally wrongful conduct".[522] In assessing proportionality, the victim state must consider the harm that was suffered and the obligation breached.[523]

The victim state can implement countermeasures that are different from the obligation breached by the responsible state. Countermeasures do not need to be symmetrical to the harm suffered and states are not limited to imposing cyber-countermeasures.[524] The United Kingdom, Germany, France, and New Zealand agree with this notion.[525]Additionally, the victim state can respond to one violation with many countermeasures. Taking such a response does not preclude the principle of proportionality.

---

517 Roy Schöndorf "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations" (2021) 9 ILS 395 at 405.

518 Draft Articles, above n 276, at 135.

519 Michael Schmitt "Germany's Positions on International Law in Cyberspace Part I" (09 March 2021) Just Security <www.justsecurity.org>.

520 Schmitt, above n 519.

521 Responsibility of States for Internationally Lawful Acts, art 51.

522 Schmitt, above n 500, at 726.

523 At 723.

524 Draft Articles, above n 276, at 129.

525 Cabinet Office (United Kingdom), above n 457. See also Federal Government of Germany, above n 109, at 13; Ministry of Armed Forces (France), above n 192, at 8; Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 2.

Rule 21 of the Tallinn Manual notes that the victim state may implement countermeasures to secure reparations.[526] A victim state will request that the hostile state end the wrongful cyber-act and make reparations for losses and potential losses.[527] For example, in 2016, North Korea allegedly carried out a cyberattack against Bangladesh's banking systems. The heist resulted in the loss of USD 81 million.[528] Bangladesh may demand North Korea to repair the cyber-infrastructures that were physically damaged by the cyberattack and repay the sum of money stolen. However, the effects of cyber-operations are difficult to quantify. If the cyberattack resulted in a significant loss of confidence in a nation's economy then it would be difficult to determine the full financial effects of the operation. Additionally, this remedy would not suffice in the face of cyber-operations that target electoral processes to undermine the political institutions of a state. Such operations incur a political cost that cannot be alleviated by financial repayments.

Yet, the law of countermeasures was a contentious issue during the 2017 UNGGE working group which failed to reach consensus on several issues. States, namely Cuba, Russia and China, objected to the notion of countermeasures in cyberspace.[529] Cuba insisted cyber-disputes were better resolved diplomatically through a multilateral settlement.[530] However, this interpretation grants cyber-aggressors an advantage because it strips the right of the victim state to respond to an internationally wrongful cyber-act.[531] Moreover, it is unlikely that a state will refrain from reacting to an internationally wrongful cyber-act taken against them.[532]

B Collective Countermeasures

Undoubtedly, countermeasures are applicable in cyberspace, but it remains unclear whether collective countermeasures are an appropriate legal response to state-sponsored cyberattacks.

526 Tallinn Manual 2.0, above n 183, at 118.

527 Delerue, above n 91, at 379.

528 Angela Moon "State-sponsored cyberattacks on banks on the rise: report" (23 March 2019) Reuters <www.reuters.com>.

529 Michael Schmitt and Liis Vihul "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms" (30 June 2017) Just Security <www.justsecurity.org> at 1.

530 At 1.

531 At 2.

532 At 2.

Some states have tried to advocate for their implementation in cyberspace, but the traditional orthodox view considers collective countermeasures unlawful.[533]

Collective countermeasures is the notion that a third state may impose countermeasures on behalf of the injured state.[534] This notion derives from the doctrine of collective self-defence.[535] However, collective self-defence is strictly limited and does not extend to the law of countermeasures.[536] Indeed, the ICJ in *Nicaragua* found that a third state could not implement countermeasures on behalf of the victim state.[537] The right to implement countermeasures was reserved for victim states and victim states alone.[538]

In 2001, the ILC discussed the applicability of collective countermeasures in accordance with the ARSIWA.[539] Article 48(1) stated that: [540]

> Any State other than an injured State is entitled to invoke the responsibility of another State in accordance with paragraph 2 if:
>
> (a) The obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or
>
> (b) The obligation breached is owed to the international community as a whole.

The provision condemns any wrongful act and demands that the responsible state rectify its breach, but it does not authorise a non-injured state to utilise enforcement powers.[541]

Special Rapporteur James Crawford argued in favour of collective countermeasures, noting that there are exceptional circumstances where they may be applied by non-injured states if the responsible state violates an obligation owed to the wider international community.[542] He noted that state practice supports the notion of collective countermeasures, citing Australia, Canada

---

533 Przemyslaw Roguski "Collective Countermeasure in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?" (2020) ICCC 26 at 27.

534 Kosseff, above n 499, at 22.

535 Visser, above n 489, at 302.

536 Samuli Haataja "'Self-defence' with the help of allies in cyberspace? Collective countermeasures and international law" (14 April 2020) Griffith University: Griffith News <https://news.griffith.edu.au>.

537 *Military and Paramilitary Activities*, above n 218, at 127.

538 Kosseff, above n 499, at 23.

539 Draft Articles, above n 276, at 126.

540 At 126.

541 Roguski, above n 533, at 29.

542 At 28.

and New Zealand's willingness to impose sanctions against Iraq, following its invasion of Kuwait in 1990.[543] For Crawford, collective countermeasures are necessary to enforce and uphold the fundamental obligations of international law without resorting to force.[544]

However, not all members of the ILC agreed with Crawford and suggested that state practice does not infer the legality of collective countermeasures in international law.[545] Serious violations of international obligations are enforced by the UNSC and not by the whim of non-injured states.[546] The UNSC has measures to prevent powerful states from exploiting the vulnerabilities of less powerful states through collective countermeasures. [547] In the end, the ILC did not explicitly deny the right to collective countermeasures and noted that this will be left to the discretion of states.[548]

The issue of collective countermeasures was deeply contentious during the drafting of ARSIWA.[549] The ILC emphasised that an agreement would not have been reached had collective countermeasures been included in the treaty.[550] Notably, Russia, China and Iran did not support the proposition and maintained that collective countermeasures would become a tool for powerful states to assert their dominance and power.[551] Others claimed that such collective action could escalate conflict and tension among states.[552] In addition, France specifically spoke out against collective countermeasures as a response to unlawful cyber-operations.[553] France noted that the current international framework did not allow for collective countermeasures and, therefore, could not be applied in the cyber-context.[554]

543 *State Responsibility – Third report on State responsibility by Mr James Crawford, Special Rapporteur* [2000] vol 2 YILC 4 at [391].
544 At [386].
545 Roguski, above n 533, at 29.
546 At 29.
547 At 30.
548 At 24.
549 At 24.
550 James Crawford "The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: A Retrospect" (2002) 96 AMJIL 874 at 884.
551 Kosseff, above n 499, at 23.
552 At 30.
553 Ministry of Armed Forces (France), above n 192, at 7.
554 At 7.

However, states recognise that they may not have adequate cyber-defences to effectively respond to malicious cyberattacks undertaken by more powerful states.[555] States may lack the necessary cyber-capabilities needed to defend against hostile aggressors that are "much larger, technologically advanced and economically more powerful".[556] Collective countermeasures may assist those states that are not technologically advanced and depend on the cyber-capabilities of third states to protect their security.[557]

Collective countermeasures can serve as an effective deterrence from future cyber-threats. The unique features of cyberspace may require a collective response. Indeed, states are densely interconnected in cyberspace. The cyber-infrastructure of one state is closely connected to the cyber-infrastructure of another state.[558] Collective countermeasures allows non-injured states to take proactive steps on behalf of an injured state. They can do this by putting in place firewalls and blocking the aggressor state from accessing its cyber-networks.[559] Collective countermeasures may serve as a legitimate practice to support small states.[560]

Furthermore, the international community has discussed the notion of collective countermeasures and whether they may be applicable in limited circumstances.[561] However, those circumstances have not been defined by international instruments or treaties. ILC members drafting ARSIWA noted that states might be persuaded to implement collective countermeasures to protect the shared goals and interests of the international community.[562]

States have debated the right of states to engage in collective countermeasures in cyberspace. President Kersti Kaljulaid of Estonia presented a speech at the 2019 CyCon Conference, publicly endorsing the right to use collective countermeasures in cyberspace:[563]

---

555 Roguski, above n 533, at 30. See Michael Schmitt "Taming the Lawless Void: Tracking the Evolution of International Law for Cyberspace" (2020) 3 TNSR 33 at 45.

556 At 26.

557 Michael Schmitt "Estonia Speaks Out on Key Rules for Cyberspace" (10 June 2019) Just Security <www.justsecurity.org>.

558 Tsagourias, above n 6, at 16.

559 Thanks to Dr. Marcin Betkier for clarifying that firewalls may not be as effective in banning whole countries and may be better suited for blocking small corporate networks.

560 Schmitt, above n 363.

561 Roguski, above n 533, at 36.

562 At 36. See Schmitt, above n 519. Schmitt claims that collective countermeasures may be "supportable under international law."

563 Kaljulaid, above n 458.

> Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation.

She held that proportionate collective countermeasures may be permitted "where diplomatic action is insufficient" and "no lawful recourse to use of force exists".[564] New Zealand also endorsed proportionate collective countermeasures for internationally wrongful acts committed by states in cyberspace.[565] Accepting such a remedy expands the legal responses open to states that have been subject to a cyberattack.

States have shared their interest in protecting the democratic functions of a nation from cyber-interference and have publicly emphasised the need to take collective action to protect those interests.[566] Though states may embrace collective countermeasures in the future, it remains an unsettled area of law in cyberspace.

C Forcible Countermeasures

While cyberattacks can produce consequences similar to kinetic weapons, targeted cyber-operations rarely include physically destructive effects.[567] Forcible countermeasures allow the victim state to take action that would violate Article 2(4) UN Charter in response to an attack that falls below the threshold of an armed attack.[568] The dissenting opinion of Judge Simma in *Oil Platforms*, finds that victim states may be able to use proportionate military measures "short of full-scale self-defence" in limited scenarios:[569]

> Against such smaller-scale use of force, defensive action - by force also "short of" Article 51 - is to be regarded as lawful. In other words, I would suggest a distinction between (full-scale) self-defence within the meaning of Article 51 against an "armed attack" within the meaning of the same Charter provision on the one hand and, on the other, the case of hostile action, for instance against individual ships, below the level of Article 51, justifying proportionate defensive measures on the

564 Kaljulaid, above n 458.

565 Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 3.

566 Laurens Cerulus "Europe Nears a Tipping Point on Russian Hacking" (03 June 2020) Politico <www.politico.eu>.

567 Lewis, above n 3. See also Emilio Iasiello "Cyber Attack: A Dull Tool to Shape Foreign Policy" (2013) ICCC 1 at 2.

568 Lotrionte, above n 76, at 93.

569 *Oil Platforms (Separate Opinion of Judge Simma)* above n 349, at 332.

> part of the victim, equally short of the quality and quantity of action in self-defence expressly reserved in the United Nations Charter.

He criticised the judgment in *Nicaragua*, noting that the threshold of an armed attack was "considerably high" leaving little recourse open to the victim state.[570] According to Judge Simma, there are exceptional circumstances where defensive action can be taken by a victim state that has been subject to a smaller-scale use of force.[571] Although, he did not define what those circumstances are or the limited range of justified responses, he added that collective self-defence would be prohibited.[572]

The reading proposed by Judge Simma was rejected by the commentators of ARSIWA, citing the exclusion of "forcible measures from the ambit of permissible countermeasures under chapter II".[573] Experts of the Tallinn Manual also noted that countermeasures did not include force.[574] While some endorsed the separate opinion of Judge Simma, the majority could not agree on the issue and therefore the rule of forcible countermeasures was not adopted.[575]

Ruys maintains that the judgement in *Nicaragua* "implicitly left open the door for proportionate forcible countermeasures".[576] Judge Yusuf of the ICJ notes that "the Court did not specify the nature of such 'countermeasures', but it could perhaps be reasonably assumed that it was referring to military countermeasures".[577] Based on his interpretation, countermeasures did not intend to exclude armed force under Article 2(4).[578] However, Corten is reluctant to accept Judge Simma's findings. He notes that such an interpretation may weaken the principles of *jus ad bellum* and lead to further ambiguities within the doctrine.[579] He maintains that there are other responses, namely enforcement measures that can be taken by the victim state, without resorting to "proportionate defensive armed measures".[580]

---

570 At 331.

571 At 331.

572 Olivier Corten "Judge Simma's Opinion in the Oil Platforms Case: To What Extent are Armed 'Proportionate Defensive Measures' Admissible in Contemporary International Law?" OUP (2011) 844 at 846.

573 Draft Articles, above n 276, at 132.

574 Tallinn Manual 2.0, above n 183, at 125.

575 At 126.

576 Ruys, above n 78, at 141.

577 Yusuf, above n 350, at 466.

578 Lotrionte, above n 76, at 94.

579 Corten, above n 573, at 845.

580 At 845.

Understandably, the narrow scope of Article 51 was intended to preserve the Charter's purpose of maintaining international peace and security.[581] However, as Dinstein noted, the requirements of necessity and proportionality can provide an adequate safeguard against the use of grave defensive force.[582] They can help protect against punitive responses and ensure that states do not abuse the right to self-defence.[583]

Depending on the cyberattack, a victim state may take forcible countermeasures in the form of: forced extradition of the individuals responsible for the cyberattack, which would be a violation of state sovereignty; targeted operations to destabilise the computers of the originating attack; or a series of DDoS attacks that cripples the attacker's ability to launch further attacks. However, forcible measures violate international law and states will have to decide whether the risk of such action is necessary to safeguard their interests.

D Non-forcible Measures

Sanctions are punitive measures designed to enforce international law.[584] Some states have chosen to implement retaliatory non-forcible measures, namely sanctions, in response to cyber-operations that target the political independence of a state. In 2015, Russia allegedly hacked into Germany's parliamentary network and stole politically sensitive material.[585] Though Russia has denied responsibility for the attacks, Chancellor Angela Merkel insisted that the evidence pointed to Russia.[586] On June 2020, Chancellor Angela Merkel urged the European Union to impose economic sanctions against Russia for its interference.[587] While it is unclear whether all 27 countries of the European Union will agree, the move by Germany indicates that sanctions may be an appropriate response to such cyberattacks.[588]

---

581 Ruys, above n 78, at 107.

582 Dinstein, above n 373, at 268.

583 At 252.

584 Malcolm Evans *International Law* (5th ed, Oxford University Press, Oxford, 2018).

585 Catherine Stupp "Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament" (11 June 2020) The Wall Street Journal <www.wjs.com> 1 at 1.

586 At 1.

587 At 1.

588 At 2. See Faesen and others, above n 214, at 22; the authors note that EU member states "mutual dependencies with Russia" will restrict their ability to implement sanctions.

Furthermore, the United States took a similar approach and imposed sanctions against Russia in response to its repeated attempts to interfere in its affairs.[589] The European Union expressed its solidarity with the United States and condemned Russia's actions by emphasising the need to "refrain from irresponsible and destabilising behaviour in cyberspace".[590] This demonstrates state willingness to implement sanctions in response to cyber-operations that target democratic institutions. It also confirms that states are not limited to the cyber-domain and may respond with non-cyber measures.[591]

E Retorsions

Retorsion is an "unfriendly but lawful measure taken in response to another State's unfriendly or unlawful act".[592] Retorsion measures are a permitted practice under international law. They may include restricting the travel access of hostile cyber-actors, expelling diplomats, or blocking state access to its servers and other cyber-infrastructures within its territory.[593]

Retorsions may help address malign cyberattacks that produce harmful effects, but which do not necessarily meet the threshold required of certain international violations.[594] The scope of retorsion is broad and faces fewer legal constraints, including its "purpose, duration and character".[595] It is not subject to the rules of proportionality and it is not confined to a particular outcome. This can be particularly attractive in cyberspace where the action does not need to be retaliatory. Yet, retorsions are limited to acts that do not violate the international obligations owed to the state.[596]

1 Expulsion

589 Gordon Corera "US imposes sanctions on Russia over cyber-attacks" (17 April 2021) BBC News <www.bbc.com>.

590 "EU expresses 'solidarity' with US over alleged Russian hacking" (16 April 2021) EURACTIV <www.euractiv.com>.

591 Schmitt, above n 500, at 726.

592 "Commentary of 2016 Article 46: Prohibition of Reprisal 2016" International Committee of the Red Cross <https://ihl-databases.icrc.org>.

593 Kosseff, above n 515, at 10.

594 At 10.

595 At 10.

596 Anderson, above n 516, at 142.

States have the sovereign authority to take retorsion measures in response to undesirable cyber-conduct.[597] A victim state will adopt this course of action to pressure the aggressor state into ceasing its malicious cyber-conduct.[598]

The most common form of retorsion in cyberspace is the expulsion of high-ranking officials and diplomats. The Russian intrusion into the 2016 United States elections had significant political consequences.[599] The United States held Russia responsible for the cyberattacks and in response, expelled 35 Russian diplomats and imposed economic sanctions.[600] The Netherland's also took a similar approach when Russian officials were accused of targeting high-tech firms and gathering intelligence on their weaponry systems. They expelled two Russian diplomats in response to the economic cyber-espionage operation.[601] In April 2021, Poland declared three Russian diplomats as *persona non grata*.[602] Interestingly, the move to expel the diplomats was not the result of a direct cyberattack against Poland but instead a response to the SolarWinds hack against the United States.[603]

The unfriendly act of expulsion can play an important role in establishing behavioural norms and deterring cyberattacks in cyberspace.[604] They can effectively demonstrate disapproval of malicious cyber-conduct, without significantly increasing the risk of escalation.

2 Public Attribution

There has been a joint effort to publicly attribute cyberattacks to the responsible state.[605] Public attribution "refers to the decision of a state to publicly attribute a cyber-operation to another state".[606] It is a national statement made by a government official acting in his or her capacity.

---

597 Kosseff, above n 515, at 10.

598 Shaw, above n 85, at 859.

599 Neil MacFarquhar "Putin, Responding to Sanctions, Orders U.S. to Cut Diplomatic Staff by 755" (30 July 2017) New York Times <www.nytimes.com>.

600 MacFarquhar, above n 600.

601 "Netherlands expels 2 Russian diplomats accused of spying" DW <www.dw.com>.

602 Joseph Conrad "Moscow Expels Three Polish Diplomats in Tit-for-tat Move" (15 April 2021) The First News <www.thefirstnews.com>.

603 Conrad, above n 604.

604 Kosseff, above n 515, at 10.

605 Duncan Hollis and Martha Finnemore "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity" (2020) 31 EJIL 970 at 971.

606 Delerue, above n 91, at 165.

This forces the accused state to confront its behaviour in cyberspace.[607] This can help shed light on the wrongful act and create a framework for appropriate state behaviour.[608]

The policy has been promoted by several states, including Germany and Estonia.[609] In fact, states publicly attribute cyber-conduct to a hostile state, even when they have not fallen victim to the cyberattack in question. To illustrate, New Zealand was not directly affected by the NotPetya cyber-operation.[610] Yet, the New Zealand Government Communications Security Bureau released a statement noting: [611]

> The GCSB's assessment found it was highly likely the Russian military General Staff Main Intelligence Directorate (GRU) was behind the campaigns and that a number of cyber proxy groups associated with these incidents are actors of the Russian state.

States accept that this process may help enforce behavioural norms and lead to conformity in existing international law in cyberspace.[612]

However, states have shied away from providing sufficient evidence when publicly assigning responsibility for cyberattacks. Thomas Bossert, Former Homeland Security Advisor to President Donald Trump, made a public statement concerning the WannaCry attacks:[613]

> After careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea. We do not make this allegation lightly. We do so with evidence, and we do so with partners. Other governments and private companies agree.

---

607 Aravindakshan, above n 4, at 288.

608 Sean Michael Kerner "What Governments Should Do to Respond to Nation State Attacks" Info Security (26 February 2020) Info-Security Group <www.infosecurity-magazine.com>.

609 Nye, above n 482, at 46.

610 "New Zealand joins international condemnation of NotPetya cyber-attack" (16 February 2018) Government Communications Security Bureau <www.gcsb.govt.nz>.

611 "Malicious cyber activity attributed to Russia" (04 October 2018) Government Communications Security Bureau <www.gcsb.govt.nz>.

612 Hollis and Finnemore, above n 606, at 975.

613 Delerue, above n 91, at 170.

Bossert did not provide any evidence to substantiate his claim and merely affirmed the support of United States allies. The concern is that public verbal condemnations are being made without sufficient evidence, undermining the legitimacy of the practice.[614]

Furthermore, this lack of evidence may provide the perpetrators with an opportunity to deny responsibility. Indeed, North Korea denied the allegations made by the United States and its allies.[615] North Korea insisted that the United States was "unreasonably accusing the DPRK without any forensic evidence."[616] While public verbal condemnation can help establish behavioural norms in cyberspace, the lack of supporting evidence can help states evade this shame and responsibility.

Understandably, states do not want to provide detailed information that may expose the vulnerabilities and capabilities of their cyber-strategy.[617] They are reluctant to disclose classified information that may risk the identity of their sources.[618] Hostile state actors can use that information to better advance their cyberattacks and prevent them from being detected in the future. Therefore, public attribution will depend on the confidence and the credibility of the victim state making that determination.[619]

There are also political obstacles that prevent public attribution from taking place. States who fall victim to a cyberattack are often hesitant to publicly admit that an attack has occurred.[620] They may not want to publicly condemn attacks to preserve their global standing, economic interest and political ties.[621] Thus, despite the evidence proving responsibility, the victim state may refuse to attribute an attack or remain silent in the face of a cyberattack. This is to avoid the political cost that can come from public attribution.[622]

614 Eichensehr, above n 317, at 567.
615 Delerue, above n 91, at 172.
616 At 172.
617 Eichensehr, above n 317, at 569. See Faesen and others, above n 214, at 28.
618 At 569.
619 Feakin, above n 443, at 2.
620 William Banks "The Bumpy Road to a Meaningful International Law of Cyber Attribution" (2019) 113 AJIL 191 at 192.
621 Eichensehr, above n 317, at 568.
622 Banks, above n 620, at 192.

In sum, this chapter looked at the way in which states may respond to a cyberattack. State practice and statements can be a useful guide when determining the legality of certain responses in cyberspace. However I acknowledge that *opinio juris* must be exercised with caution. As Andrew Guzman notes, "powerful states dominate the question of state practice".[623] It is states that have well-established cyber-technologies that dominate the field of cyberspace.[624] In light of this, I recognise the limitations of such responses in cyberspace.

VIII Looking Forward

Cyberspace is a dynamic, fluid and novel environment. How states choose to apply the principles of *jus ad bellum* can be very subjective. This subjectivity is further heightened in the field of cyberspace because of the degree of knowledge required to detect and attribute an incoming cyberattack.

Currently, no international cyber-treaty exists and the UNGGE has struggled to consistently reach consensus over the years. States and the wider international community have generally accepted that the principles of *jus ad bellum* can apply to cyber-operations, but the legal boundaries of how it can apply remains blurred.[625] Cuba, China and Russia are of the view that self-defence cannot be invoked in cyberspace and that a new regulatory framework is required to address the unique effects of cyber-operations.[626] Russia accepts that international law applies in cyberspace but adds that a globally binding treaty can ensure certainty and stability. China supports the demilitarisation of cyberspace and explains that a "cyber arms control" agreement is necessary to prevent national security threats in cyberspace.[627] Cuba, China and Russia warn against the continuing militarisation of cyberspace.[628] Cuba notes that information technology is a tool "to promote peace, not to promote war, the use of force, interventionism, destabilization, unilateralism or terrorist actions".[629]

---

623 Andrew Guzman "Saving Customary International Law" (2005) 7 MJIL 116 at 151

624 Roscini, above n 277, 125.

625 Anders Henriksen "The end of the road for the UN GGE process: The future regulation of cyberspace" (2019) 5 JOC 1 at 1.

626 Waxman, above n 446, at 115.

627 Rid, above n 31, at 35.

628 Ann Väljataga "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly" (2017) CCDCOE <https://ccdcoe.org>.

629 Miguel Rodríguez, Representative of Cuba "Final Session of Group of Governmental Experts of Developments in the Field of Information and Telecommunication in the Context of International Security" (United Nations, New York, 23 June 2017).

On the other hand, the United States maintains that cyberspace is best governed by existing international law. They refuse to support a cyber-treaty that may embolden repressive state practices.[630] Therefore, a cyber-treaty will be difficult to draft, adopt and enforce because it requires the cooperation and agreement of states that share different priorities, views and interests in cyberspace.[631] It will require 193 Member States to come together to establish a uniform international legal regime in cyberspace.

However, cyber-technology is rapidly developing and the risk of cyber-conflict is becoming more of a reality for states. While states may benefit from a universal cyber-treaty, there is no appetite for it. Waiting for a universal cyber-treaty may impede effective cooperation to combat cyber-threats.[632] For this reason, a regional cyber-treaty is more productive in developing international cyber-norms.

A Regional Cyber-Treaty

Cyberspace carries with it global security threats and it is imperative for states to engage multilaterally in this field.[633] A regional cyber-treaty may help bring like-minded states together to develop a clearer narrative of cyber-norms.[634]

Regional states are highly interdependent and their economic growth often depends on the financial and political stability of border-states. States are more likely to be dissuaded from launching cyberattacks if they have strong economic and regional ties with other states.[635] In 2018, the Association of Southeast Asian Nations (ASEAN) endorsed the non-binding principles outlined in the 2015 UNGGE report. The leaders sought to improve cyber-stability

630 *Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race* GA/DIS/3560 (2016).

631 Sam Sachdeva "NZ's line in the sand on cyberattacks" (07 December 2020) Newsroom <www.newsroom.co.nz>.

632 Nataliya Maroz "Regionalization of International Cooperation in the Fight Against Cyber Crime" (2019) 10 LR 218 at 219. See also Crootof, above n 650, at 640.

633 Gary Waters "The Case for a Regional Cyber Security Action Task Force" (2011) 7 SC 1 at 1.

634 Joyce Hakmeh and Alison Peters "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free and Secure Internet" (13 January 2020) Council on Foreign Relations <www.cfr.org>.

635 Nye, above n 482, at 59.

and secure confidence-building measures in the Asia-Pacific.[636] They noted the need to support "regional initiatives for international cooperation towards cybersecurity".[637]

The UNGGE consultations can form the basis of regional negotiations and treaties. For example, the Singapore-ASEAN Cybersecurity Centre of Excellence aims to advance regional cyber-cooperation by strengthening technical assistance and encouraging "open-source information sharing". This goal is consistent with the 2015 UNGGE consensus report which recognised the technical disparity between states and "called for the international community to assist in improving the security" of cyber-infrastructures. Thus, states do not have to begin from scratch, they can rely and build on existing global cyber-norms.[638]

In my opinion, a regional treaty should include legal provisions that support the extradition of patriotic cyber-actors. The treaty should emphasise an extradition clause to ensure that individuals who commit cyberattacks are extradited and tried within the jurisdiction of the victim state. This is an important legal criterion for cooperation and enforcement of cyber-norms.[639] States should support a procedure of punishment for individuals who launch malicious cyberattacks within their territory.[640] A provision of this kind will prevent states from providing safe havens for patriotic cyber-actors and ensure that individuals are held responsible for their malicious cyber-activities.[641]

There is a global desire for stability in cyberspace, however, the means to get there differ between states. I recognise that catering to the unique requirements and needs of a particular region may hinder global consensus efforts in cyberspace.[642] The different approaches and

---

636 Christy Un "It's time for the Asia-Pacific to Move toward Regional Cyber Norms" (14 October 2020) The Diplomat <https://thediplomat.com>.

637 *Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* GA Res 73/266 (2019).

638 Wolfgang Kleinwächter "International Law and Cyberspace: It's the "How", Stupid" (10 December 2020) CircleID <www.circleid.com>.

639 Maroz, above n 632, at 221. But see Faesen and others, above n 214, at 29. They argue that such indictments may be risky because the accused state has the right to request sensitive information from the prosecuting state in order to defend itself. This may compromise the national security interests of the victim state.

640 At 223.

641 At 223.

642 At 219.

different cyber-treaties may lead to inconsistencies in the implementation of cyber-norms. It may further confuse states or affect the progress being made in the field of cyberspace.[643] However, the 2015 UNGGE Report can serve as a baseline of minimum requirements and help unite existing narratives.[644]

Additionally, it may be difficult to regulate and enforce regional cyber-treaties. Organisations that have drafted similar cyber-treaties have seen them fall apart during implementation or fail to gather full regional support.[645] For example, in 2014, the African Union (AU) established the Convention on Cyber Security and Personal Data Protection.[646] The legal framework included measures that would protect personal data and prohibit cyber-activities that would violate the security or integrity of critical information infrastructures.[647] Yet, only 14 of the 55 AU members signed the treaty and only eight have ratified it.[648] Nonetheless, regional cooperation and enforcement may help to establish a secure cyberspace model and clarify international cyber-norms.[649] Relying exclusively on soft-law instruments may discourage international collaboration.

B Independent Agency of Attribution

After examining the challenges of cyber attribution, I propose that a centralised international platform should be introduced to assign responsibility to cyber-actors of hostile cyber-activities.[650] In order to conclude responsibility, this global institution would be in charge of investigating cyberattacks, facilitating information-sharing networks and providing independent assistance to states and international legal forums.[651]

643 At 219.

644 Un, above n 636.

645 Uchenna Jerome Orji "The African Union Convention on Cyber Security: a Regional Response towards Cyber Stability" 12 MUJLT 91 at 93.

646 African Union Convention on Cyber Security and Personal Data Protection (opened for signature 27 June 2014).

647 Orji, above n 645, at 94.

648 "African Union Convention on Cyber Security and Personal Data Protection" (11 May 2020) African Union <https://au.int>.

649 Joyce Hakmeh and Alison Peters "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free and Secure Internet" (13 January 2020) Council on Foreign Relations <www.cfr.org>.

650 Eichensehr, above n 317, at 588. See generally Rebecca Crootof "International Cybertorts: Expanding State Accountability in Cyberspace" (2018) 103 CLR 565 at 637.

651 Mueller and others, above n 338, at 115

Encouraging behavioural norms of information sharing will lead to more accurate determinations in cyberspace. As *Nicaragua* correctly noted, "the problem is not… the legal process of imputing the act to a particular state… but the prior process of tracing material proof of the identity of the perpetrator".[652] This is especially true in cyberspace, where cyberattacks can be launched from several computer networks in different states.[653] The agency will encourage states to share and handover evidence of cyberattacks that originate from their cyber-infrastructure.[654] This process of collaboration and cross-checking will increase the accuracy of liability and accountability in cyberspace.

Advocates of this approach have outlined several proposals on how this agency may function. Microsoft points to the success of the IAEA and argues for a multi-stakeholder approach with "a diverse set of nation-states and geographic regions".[655] On the other hand, the Rand Corporation, a non-governmental global policy think-tank tasked with researching United States national security, maintains that member states must be excluded to ensure the legitimacy of its institutions and attributions.[656] According to the Corporation, state representatives may manipulate the agency and provide biased information to serve its political objective.[657] This can taint the credibility of the organisation and the reliability of its investigations. Instead, the body should be composed of non-state experts.[658]

However, to provide effective and efficient determinations, membership must include state representatives.[659] State representatives can report cyberattacks and hand over relevant information to the organisation. Other members of the organisation, including technical forensic experts, scholars, and civil society, can help analyse and vet biased information provided by states. The nature of cyberspace means that collaboration, engagement and evidence sharing are required to ensure effective and efficient determinations.[660]

---

652 Tsagourias, above n 187, at 234.

653 Eva-Nour Repussard "There Is No Attribution Problem, Only a Diplomatic One" (22 March 2020) E-International Relations <www.e-ir.info>.

654 Eichensehr, above n 317, at 588.

655 At 596.

656 John Davis and others "Stateless Attribution: Toward International Accountability in Cyberspace" Rand Corporation <www.rand.org> at 29.

657 At 30.

658 At 29.

659 At 31.

660 Tsagourias and Farrell, above n 314, at 959.

Furthermore, states that do not have the necessary cyber-capabilities to make or disprove attribution claims can seek assistance from the agency. Victims of cyberattacks "either cannot afford cyber attribution assistance or do not know where to turn to for help".[661] This can help ease the burden on states that are more vulnerable to cyberattacks but are not technologically advanced enough to verify attribution claims.

However, the construction of such an agency has not evaded criticism. Tsagourias and Farrell correctly note that "the effectiveness of such an agency will depend on the willingness of states to cooperate and accept its findings".[662] Firstly, states may refuse to share information and deny the agency access to its computer networks.[663] Secondly, assigning responsibility is believed to fall within the sovereign powers of the state. Many states accept no obligation to provide sufficient evidence when attributing a cyberattack to a state.[664] In 2016, Former State Department Legal Adviser Brian Egan, explained that:[665]

> Despite the suggestion by some States to the contrary, there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action. There may, of course, be political pressure to do so, and States may choose to reveal such evidence to convince other States to join them in condemnation, for example. But that is a policy choice—it is not compelled by international law.

In 2018, England's Attorney General, Jeremy Wright affirmed Egan's statement.[666] More recently, New Zealand asserted that "while any legal attribution should be underpinned by a sound evidential basis, there is no general obligation on the attributing state to disclose that basis".[667]

Finally, accepting the agency's findings may require a change in state behaviour and the application of international law. To demonstrate, legal responses, including self-defence and countermeasures, lose their justification once significant time has passed.[668] Since attributing

661 Eichensehr, above n 317, at 590.
662 Tsagourias and Farrell, above n 314, at 960.
663 At 960.
664 At 960.
665 Eichensehr, above n 463.
666 Eichensehr, above n 317, at 546.
667 Ministry of Foreign Affairs and Trade (New Zealand), above n 89, at 4.
668 Tsagourias and Farrell, above n 314, at 961.

responsibility in cyberspace requires a thorough investigation, the agency may be unable to produce a determination in due time.[669] Consequently, states may grow frustrated awaiting attribution determinations, leading them to make their own determinations.

It will be difficult to establish an operational framework of this kind. Indeed, it is unclear whether the agency should fall within an existing body or whether it should function separately. It is also unclear whether membership should explicitly exclude states.

Nonetheless, as cyberattacks become more common and more disruptive, the international community will have to consider an appropriate framework for cyber attribution. In the absence of a clearly defined evidentiary standard of proof, the agency may help create certainty and validity of cyber attribution. It can secure the legitimacy of accusations, improve public confidence and enhance the trust of our allies.[670]

IX Conclusion

The UN Charter is a living document that continues to evolve and adapt to meet the needs of the international community.[671] However the principles of *jus ad bellum* presents a unique set of challenges in cyberspace. For example, if a foreign government wanted to interfere with a nation's democratic elections, it could launch a missile strike targeting the voting stations of a state. An attack like this would clearly violate Article 51 UN Charter because of its physically destructive effects. It would also be much easier to attribute and therefore much easier to respond to. By contrast, a cyberattack could change voter registration details or alter votes on voting machines. A cyberattack of this kind would be much more difficult to respond to because it would not produce any observable physical destruction and is more difficult to detect and attribute due to the anonymity afforded by cyberspace. Arguably, the cyberattack would also be more effective.

This dissertation attempted to demonstrate that traditional understanding of *jus ad bellum* fails to acknowledge the non-physical consequences of cyber-operations.[672] To date, most cyber-

669 At 961.
670 Eichensehr, above n 317, at 578.
671 Ruys, above n 2, at 163.
672 Melzer, above n 80, at 6.

weapons have been used to conduct small-scale operations that disrupt and undermine the cyber-functions of political or financial institutions.[673] Yet, laws governing cyber-force and cyber armed attack has been interpreted to require physical effects. Additionally, the dictatorial features of coercion do not adequately address the unique effects of most cyber-operations.[674]

The technological features of cyberattacks may require a re-evaluation of state behaviour. Cyberattacks are subtle, which makes it difficult to assess when and how a victim state may respond to a cyberattack.[675] International law's understanding of what is a necessary, what is immediate, and what is proportionate, will require further assessment in cyberspace. Additionally, the anonymity and accessibility of cyberspace make it difficult to attribute with great certainty and accuracy.[676] Indeed, states may delay taking forcible action to ensure that the correct attacker has been identified, that the attack has crossed the necessary threshold and that there are no other responses open to the victim state.

To address the shortfalls of the Charter in cyberspace, I recommend that continuous and repeated disruption of a cyber-network should be classified as an unlawful incursion. I argue for a reconceptualisation of cyber-coercion to address electoral cyber-interference. I adopt the standard of circumstantial evidence to attribute low-intensity cyber-operations. Circumstantial evidence can account for the unique characteristics of cyberspace and help address some of the difficulties of obtaining and analysing evidence in cyberspace. States should uphold a standard of due diligence in cyberspace. While they cannot regulate the online behaviour of all citizens, once they have been made aware of a cyberattack, they must take all practical steps necessary to end the operation.

The unlikelihood of a universal cyber-treaty means that the development of new cyber-rules will depend on the shared views, experiences, and behaviours of states in cyberspace. It will be interesting to examine the development of new rules as smaller states enter this discussion. The development of new rules will depend on collaboration, transparency and engagement among all UN states. A regional cyber-treaty followed by an independent operational

673 Schmitt, above n 512, at 698.
674 Ruys, above n 2, at 171.
675 At 171.
676 Roscini, above n 336, at 234.

framework to determine attribution of state-sponsored cyberattacks, will help aid those efforts and enhance the legitimacy of state responses in cyberspace.

BIBLIOGRAPHY

I PRIMARY SOURCES

A International Instruments

- *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgement)* ICJ [2005] Rep 168.
- African Union Convention on Cyber Security and Personal Data Protection (opened for signature 27 June 2014).
- *Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race* GA/DIS/3560 (2016).
- *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgement)* ICJ [2007] Rep 43.
- Charter of the United Nations (opened for signature 26 June 1945, entered into force 24 October 1945).
- *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, GA Res 58/199, A/RES/58/199 (2004).
- *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania) (Merits)* [1949] ICJ Rep 3.
- *Developments in the field of information and telecommunications in the context of international security* GA Res 73/27, A/Res/60/1 (2018).
- *Eritrea Ethiopia Claims Commission, Partial Award, Jus ad Bellum, Ethiopia's Claims* 1–8, The Hague, [2005].
- *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* GA Res 70/174, A/Res/70/174 (2015).
- International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976).
- *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226.

- *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* GA Res 69/723, A/69/723 (2015).
- Letter from Daniel Webster (United States Secretary of State) to Lord Ashburton regarding the *Caroline* case (6 August 1842).
- *Non-interference in the internal affairs of States* GA Res 31/91, A/31/414 (1976).
- *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) (Merits)* [1986] ICJ Rep 14.
- *Gabčíkovo-Nagymaros Project (Hungary/Slovakia) (Judgments)* [1997] ICJ Rep 7.
- *Open-ended working group on developments in the field of information and telecommunications in the context of international security* A/AC.290/2021/CRP.2 (2021).
- *Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [2003] ICJ Rep 161.
- *Prosecutor v Tadić (Judgment)* ICTY Appeals Chamber IT-94-1-A, 15 July 1999.
- *Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* GA Res 73/266 (2019).
- *Responsibility of States for Internationally Lawful Acts (Commentary)* GA Res 56/83, A/Res/56/83 (2001).
- *Report of the Special Committee on Friendly Relations and Co-operation among States* A/7326 (1969).
- *Special Committee on Principles of International Law concerning Friendly Relations and Co-operation among States* A/AC.125/SR.110 to 114 (1970).
- SC Res 678, S/Res/678 (1990).
- SC Res 502, S/Res/502 (1982).
- *State Responsibility – Third report on State responsibility by Mr James Crawford, Special Rapporteur* [2000] vol 2 YILC 4 at [391].
- *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States* GA RES 2625 XXV A/Res/2625 (1970).
- U.S.–China Cyber Agreement United States-China (signed 25 September 2015) entered into force 25 September 2015.

- *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) (Judgment)* [1980] ICJ Rep 3.

II SECONDARY SOURCES

A Books

- William H Boothby "Cyber weapons: oxymoron or a real world phenomenon to be regulated?" in Karsten Friis and Jens Ringsmose (ed) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (Routledge, London, 2016).
- D.W Bowett *Self-Defence in International Law* (Manchester University Press, Manchester, 1958).
- Ian Brownlie *International Law and the Use of Force by States* (Oxford University Press, New York, 1963).
- Russell Buchan *Cyber Espionage and International Law* (Oxford Hart Publishing, Oxford, 2019).
- Olivier Corten *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart Publishing, London, 2010).
- François Delerue *Cyber Operations and International Law* (Cambridge University Press, Cambridge, 2020).
- Yoram Dinstein *War, Aggression and Self-defence* (6th ed, Cambridge University Press, Cambridge, 2017).
- Malcolm Evans *International Law* (5th Ed, Oxford University Press, Oxford, 2018).
- Binxing Fang *Cyberspace Sovereignty: Reflections on Building a Community of Common future in Cyberspace* (Springer, Singapore, 2018).
- Carlo Focarelli "Self-defence in Cyberspace" in Nicholas Tsagourias and Russell Buchan (eds*) Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, Cheltenham, 2015).
- Judith Gardam *Necessity, Proportionality and the Use of Force by States* (Cambridge University Press, Cambridge, 2004).
- Christine Gray *International Law and the Use of Force* (3rd Ed, Oxford University Press, Oxford, 2008).

- James Green *The International court of Justice and Self-Defence in International Law* (Hart Publishing Ltd, Portland, 2009).
- Daniel Kuehl "From Cyberspace to Cyberpower: Defining the Problem" Franklin D. Kramer and others (ed) *Cyberpower and National Security* (University of Nebraska Press, Washington D.C, 2009).
- Georg Nolte Albrecht Randelzhofer "Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51" in Bruno Simma, and others (ed) *The Charter of the United Nations (3rd Edition): A Commentary, Volume II* (Oxford University Press, Oxford, 2012).
- William Owens and others *Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press, Washington D.C, 2009).
- Thomas Rid *Cyber War Will Not Take Place* (C. Hurst Publishers Limited, Hurst, 2013).
- Anna Riddell and Brendan Plant *Evidence before the International Court of Justice* (British Institute of International and Comparative Law, London, 2009).
- Przemyslaw Roguski "Violation of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach" Dennis Broeders and Bibi van den Berg (ed) *Governing Cyberspace Behaviour, Power, and Diplomacy* (Rowman & Littlefield Publishers, London, 2020).
- Nicholas Tsagourias "The Legal Status of Cyberspace" in Nicholas Tsagourias and Russell Buchan (eds*) Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, Cheltenham, 2015).
- Marco Roscini *Cyber Operations and the Use of Force in International Law* (Oxford University Press, Oxford, 2014).
- Tom Ruys *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge University Press, New York, 2010).
- Michael Schmitt *Essays on Law and War at the Fault* (TMC Asser Press Springer, The Hague, 2012).
- Michael N Schmitt *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).
- Michael N Schmitt *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

- Michael N Schmitt "The Use of Cyber Force and International Law" in Marc Weller (ed) *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, Oxford, 2016).
- Walter Sharp *Cyberspace and the Use of Force* (Aegis Research Corporation, Virginia, 1999).
- Malcolm Shaw *International Law* (8th ed, Cambridge University Press, New York, 2017).
- Kinga Tibori Szabó *Anticipatory Action in Self-Defence* (T. M. C. Asser Press, The Hague, 2011).
- Kim Zetter *Countdown to Zero Day* (Crown Publishers, New York, 2014).

B Journal Articles

- Collin Allan "Attribution Issues in Cyberspace" (2013) 13 CKJICL 55.
- Sahar Alshathry "Cyber Attack on Saudi Aramco" (2017) 11 IJMIT 3307 at 3037.
- Troy Anderson "Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals" (2016) 34 AJICL 136 at 148.
- Sharngan Aravindakshan "Cyberattacks: a look at evidentiary threshold in International Law" (2020) IJIL 286.
- William Banks "The Bumpy Road to a Meaningful International Law of Cyber Attribution" (2019) 113 AJIL 191.
- William H Boothby "Methods and Means of Cyber Warfare" (2013) 89 ILS 387.
- Gary Brown and Keira Poellet "The Customary International Law of Cyberspace" (2012) 6 SSQ 126.
- Russell Buchan "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" (2012) 17 JCSL 211.
- Geoffrey DeWeese "Anticipatory and Pre-emptive Self-Defense in Cyberspace: The Challenge of Imminence" AOC (2015) 81.
- Kristen Eichensehr "The Law and Politics of Cyberattack Attribution" (2020) 67 UCLA L Rev. 558.
- Mette Eilstrup-Sangiovanni "Why the World Needs an International Cyberwar Convention" (2017) 31 PT 380.

- Sina Etezazian "The nature of the self-defence proportionality requirement" (2016) 3 UFIL 260.
- Louk Faesen and others "Case Study: Protecting Electoral Infrastructure from Russian Cyberoperations (2020) HCSS 16.
- David Fidler "Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection" (2015) GJLA 8.
- Dieter Fleck "Searching for International Rules Applicable to Cyber Warfare – A critical First Assessment of the New Tallinn Manual" (2013) 18 JCSL 331
- James Green "The 'additional' criteria for collective self-defence: request but not declaration" (2017) 4 UFIL 4.
- Francis Grimal and Jae Sundaram "Cyber Warfare and Autonomous Self-defence" (2017) 4 JUFIL 313.
- Andrew Guzman "Saving Customary International Law" (2005) 7 MJIL 116.
- Samuli Haataja and Afshin Akhtar-Khavar "Stuxnet and international law on the use of force: an informational approach" (2018) 7 CILJ 99 at 107.
- Monica Hakimi and Jacob Katz Cogan "The Two Codes on the Use of Force" (2016) 27 EJIL 257.
- Richard Hanania "Norms Governing the Interstate Use of Force: Explaining the Status Quo Bias of International Law" (2013) 27 EL 831.
- Oona A Hathaway "The Drawback and Dangers of Active Defense" (2014) ICCC 39.
- Oona A Hathaway and others "The Law of Cyber-Attack" (2012) 100 CLR 817.
- Ryan Hayward "Evaluating the 'Imminence' of a Cyber Attack for Purposes of Anticipatory Self-Defense" (2017) 117 CLR 399.
- Christian Henderson "The use of cyber force: Is the jus ad bellum ready?" (2016) 27 QIL 3.
- Louis Henkin "The Reports of the Death of Article 2(4) Are Greatly Exaggerated" (1971) 65 AJIL 544.
- Anders Henriksen "The end of the road for the UN GGE process: The future regulation of cyberspace" (2019) 5 JOC 1.
- Duncan Hollis and Martha Finnemore "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity" (2020) 31 EJIL 970.
- John Hargrove "The Nicaragua Judgment and the Future of the Law of Force and Self-defense" (1987) 81 AJIL 135.

- Emilio Iasiello "Cyber Attack: A Dull Tool to Shape Foreign Policy" (2013) ICCC 1.
- Uchenna Jerome Orji "The African Union Convention on Cyber Security: a Regional Response towards Cyber Stability" 12 MUJLT 91.
- Christopher Joyner and Catherine Lotrionte "Information Warfare as International Coercion: Elements of a Legal Framework" (2001) 12 EJIL 825.
- Agata Kleczkowska "When 'the Use of Force is Prohibited? – Article 2(4) and the 'Threshold' of Use of Force" (2019) 8 AMULR 110.
- Tobias Kliem "You can't cyber in here, this is the War Room! A rejection of the effects doctrine on cyberwar and the use of force in international law" (2017) 4 RTFG 344.
- Id Kilovaty "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information" (2018) 9 HNSJ 146.
- Chris Kinslow "Game of Code: The Use of Force against Political Independence in the Cyber Age" (2018) 4 AL 29.
- Jeff Kosseff "Retorsion as a Response to Ongoing Malign Cyber Operations" (2020) ICCC 9.
- Jeff Kosseff "Collective Countermeasures in Cyberspace" (2020) 10 JICL 18.
- David Kretzmer "The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum" (2013) 24 EJIL 23.
- Sarah Kreps and Jacqulyn Schneider "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics" (2019) 5 JCS 1.
- Henning Lahman "Information Operations and the Question of Illegitimate Interference under International Law" (2020) 53 ILR 189.
- Jarno Limnéll "Proportional Response to Cyberattacks" (2017) 1 CIS 37.
- Herbert Lin "Attribution of Malicious Cyber Incidents From Soup to Nuts" (2016) NSTL 1.
- Catherine Lotrionte "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law" (2018) 3 CDR 78.
- Nataliya Maroz "Regionalization of International Cooperation in the Fight Against Cyber Crime" (2019) 10 LR 218.
- Eric Mejia "Act and Actor Attribution in Cyberspace A Proposed Analytical Framework" (2014) 8 SSQ 114.

- Thibault Moulin "Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward" (2020) JCSL 1.
- Harriet Moynihan "The vital role of international law in the framework for responsible state behaviour in cyberspace" (2020) JCP 1.
- Milton Mueller and others “Cyber Attribution: Can a New Institution Achieve Transnational Credibility” (2019) CDR 107.
- Colleen Newbill "Defining Critical Infrastructure for a Global Application" (2019) 26 IJGLS 761.
- Reese Nguyen "Navigating "Jus Ad Bellum" in the Age of Cyber Warfare" (2013) 101 CLR 1079.
- Joseph Nye Jr. "Deterrence and Dissuasion in Cyberspace" (2017) 41 MIT 44.
- Mary Ellen O'Connell "The True Meaning of Force: A Further Response to Tom Ruys in the Interest of Peace" (2014) 108 ASIL 153.
- Jens Ohlin "Did Russian Cyber Interference in the 2016 Election Violate International Law?" (2017) 95 TLR 1580.
- Przemyslaw Roguski, "Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?" (2020) ICCC 26.
- Marco Roscini "World Wide Warfare – Jus ad Bellum and the Use of Cyber Force" (2010) 14 MPYUL 86.
- Marco Roscini "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations" (30 June 2014) 50 Texas Intl LJ 233.
- Tom Ruys "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?" (2014) AJIL 159.
- Oscar Schachter "The Right of States to Use Armed Force" (1984) 82 MLR 1620.
- Oscar Schachter "In Defense of International Rules on the Use of Force" (1986) 53 UCLR 113.
- Michael Schmitt ""Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law" (2014) 54 VJ Intl L 698.
- Michael Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" (2010) 54 HILJ 14.
- Roy Schöndorf "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations" (2021) 9 ILS 395.

- Paulo Shakarian "The 2008 Russian Cyber-Campaign Against Georgia" (2011) Military Review 63.
- Glenn Sulmasy and John Yoo "Counterintuitive: Intelligence Operations and International Law" (2007) 28 MJ Intl Law 625.
- Nicholas Tsagourias and Michael Farrell "Cyber Attribution: Technical and Legal Approaches and Challenges" (2020) 31 EJIL 941.
- Nicholas Tsagourias "Cyber Attacks, Self-defence and the Problem of Attribution" (2012) 17 JCSL 229.
- Laura Visser "Intervention by invitation and collective self-defence: two sides of the same coin?" (2020) 7 JFIL 292.
- Gary Waters "The Case for a Regional Cyber Security Action Task Force" (2011) 7 SC 1.
- Sean Watts "Low Intensity Cyber Operations and the Principle of Non-Intervention" (2014) 14 BYIL 137.
- Matthew Waxman "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions" (2013) 89 Intl L Stud 109.
- David Weissbrodt "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage" (2013) 22 NJIL 347.
- Abdulqawi A Yusuf, "The Notion of Armed Attack in the Nicaragua Judgment and Its Influence on Subsequent Case Law" (2012) 25 LJIL 461.

C Internet Materials

- "2019 International Law Supplement" (2019) Australia's International Cyber Strategy <www.dfat.gov.au>.
- "Advancing Cyber Stability" (November 2019) Global Commission on the Stability of Cyberspace <https://cyberstability.org>.
- "African Union Convention on Cyber Security and Personal Data Protection" (11 May 2020) African Union <https://au.int>.
- "Commentary of 2016 Article 46: Prohibition of Repraisal 2016" International Committee of the Red Cross <https://ihl-databases.icrc.org>.
- "EU expresses 'solidarity' with US over alleged Russian hacking" (16 April 2021) EURACTIV <www.euractiv.com>.

- "General Staff of Iranian Armed Forces Warns of Tough Reaction to any Cyber Threat" (18 August 2020) <https://nournews.ir>.
- "Malicious cyber activity attributed to Russia" (04 October 2018) Government Communications Security Bureau <www.gcsb.govt.nz>.
- "Netherlands expels 2 Russian diplomats accused of spying" DW <www.dw.com>.
- "New Zealand joins international condemnation of NotPetya cyber-attack" (16 February 2018) Government Communications Security Bureau <www.gcsb.govt.nz>.
- "North Korea's Offensive Cyber Program Might Be Good, But Is it Effective?" (25 October 2017) Council on Foreign Relations <www.cfr.org>.
- "Understanding Server Traffic logs and detecting Denial of Service Attacks" Microsoft <https://techcommunity.microsoft.com>.
- Australian Government Department of Foreign Affairs and Trade "Australia's International Cyber Engagement Strategy" (October 2017) Australian Government Department of Foreign Affairs and Trade <www.dfat.gov.au>.
- Cabinet Office (United Kingdom) "Policy Paper: Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy" (16 March 2021) GOV.UK <www.gov.uk>.
- Department of Homeland Security "The National Strategy to Secure Cyberspace" (February 2003) Cybersecurity and Infrastructure Security Agency <https://us-cert.cisa.gov>.
- Department of the Prime Minister and Cabinet "New Zealand's Cyber Security Strategy 2019" (July 2019) DPMC <https://dpmc.govt.nz>.
- Department of United States of America "U-2 Overflights and the Capture of Francis Gary Powers 1960" Office of the Historian Office of the Historian <https://history.state.gov>.
- European Commission "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation" (March 2018) Publication Office of the EU <https://op.europa.eu>.
- Ministry of Armed Forces (France) "International Law Applied to Operations in Cyberspace" (October 2019) Ministère des Armées <www.defense.gouv.fr>.
- Ministry of Foreign Affairs (Netherlands) "International Law in Cyberspace" Government of the Netherlands <www.government.nl>.

- Ministry of Foreign Affairs and Trade (New Zealand) "The Application of International Law to State Activity in Cyberspace" (01 December 2020) New Zealand Foreign Affairs and Trade <www.mfat.govt.nz>.
- Ministry of Foreign Affairs Finland "International law and cyberspace: Finland's national positions" (19 October 2020) Finnish Government <https://valtioneuvosto.fi>.
- Ministry of Information and Communications Technology "Qatar National Cyber Security Strategy" (May 2014) MOTC <https://www.motc.gov.qa>.
- Abigail Abrams "Here's What We Know So Far About Russia's 2016 Meddling" (18 April 2019) Times <www.time.com>.
- Dapo Akande "The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?" (17 March 2018) EJIL Talk! <www.ejiltalk.org>.
- Saira Asher "What the North Korean internet really looks like" (21 September 2016) BBC News <www.bbc.com>.
- Clara Assumpção "The Problem of Cyber Attribution Between States" (06 May 2020) E-International Relations <www.e-ir.info>.
- Jonathan Berr ""WannaCry" ransomware attack losses could reach $4 billion" (16 May 2017) CBS News <www.cbsnews.com>.
- Erica Borghard and Jacquelyn Schneider "Russia's Hack Wasn't Cyberwar. That Complicates US Strategy" (17 December 2020) Wired < www.wired.com>.
- General James E Cartwright "Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates: Joint Terminology for Cyberspace Operations" (November 2011) Homeland Security Digital Library <www.hsdl.org>.
- Martin Chulov "Israel appears to confirm it carried out cyberattack on Iran nuclear facility" (11 April 2021) The Guardian <www.theguardian.com>.
- Gil Baram and Kevjn Lim "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks" (5 June 2020) Foreign Policy <https://foreignpolicy.com>.
- Laurens Cerulus "Europe Nears a Tipping Point on Russian Hacking" (03 June 2020) Politico <www.politico.eu>.
- Christopher Chivvis and Cynthia Dion-Schwarz "Why It's So Hard to Stop a Cyberattack — and Even Harder to Fight Back" (30 March 2017) Rand Cooperation <www.rand.org>.

- Joseph Conrad "Moscow Expels Three Polish Diplomats in Tit-for-tat Move" (15 April 2021) The First News <www.thefirstnews.com>.
- Gordon Corera "US imposes sanctions on Russia over cyber-attacks" (17 April 2021) BBC News <www.bbc.com>.
- Dapo Akende "Oxford Statement on International Law Protections against Foreign Electoral Interference through Digital Means" (28 October 2020) Just Security <www.justsecurity.org>.
- Claus Kress "On the Principle of Non-Use of Force in Current International Law" (30 September 2019) Just Security <www.justsecurity.org>.
- John Davis and others "Stateless Attribution: Toward International Accountability in Cyberspace" Rand Corporation <www.rand.org>.
- Colin Dwyer "Pompeo Says Russia 'Pretty Clearly' Behind Cyberattack, Prompting Pushback From Trump" (19 December 2020) NPR <www.npr.org>.
- Kristen Eichensehr "Cyberattack Attribution and International Law" (24 July 2020) Just Security <www.justsecurity.org>.
- Kristen Eichensehr "Political Parties as Critical Infrastructure?" (22 June 2017) Just Security <www.justsecurity.org>.
- Tobias Feakin "Developing a Proportionate Response to a Cyber Incident" (August 2015) Council of Foreign Policy <https://cdn.cfr.org>.
- Sam Frizell "Here's What Chinese Hackers Actually Stole From U.S. Companies" (20 May 2014) Times <https://time.com>.
- Josh Fruhlinger "Malware explained: How to prevent, detect and recover from it" (17 May 2019) CSO <www.csoonline.com>.
- Josh Fruhlinger "Viruses explained: How they spread and 5 signs you've been infected" (16 July 2019) CSO <www.csoonline.com>.
- Ryan Goodman "Cyber Operations and the U.S. Definition of "Armed Attack"" (08 March 2018) Just Security <www.justsecurity.org>.
- Ryan Goodman "International Law and the US Response to Russian Election Interference" (05 January 2017) Just Security <www.justsecurity.org>.
- Joe Gould "US Cyber Commander: Hackers Will 'Pay a Price'" (11 May 2015) Defense News <www.defensenews.com>.

- Samuli Haataja "'Self-defence' with the help of allies in cyberspace? Collective countermeasures and international law" (14 April 2020) Griffith University: Griffith News < https://news.griffith.edu.au>.
- Ben Hubbard and others "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran" (14 September 2019) New York Times <www.nytimes.com>.
- Lindsay Hughes "Israel vs. Iran: The Deadly Cyberattacks Continue" Future Directions International (01 July 2020) <www.futuredirections.org.au>.
- Brian Humphreys "The Designation of Election Systems as Critical Infrastructure" (18 September 2019) Congressional Research Service <https://crsreports.congress.gov>.
- Jeh Johnson "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector" (06 January 2017) Homeland Security <www.dhs.gov>.
- Sean Michael Kerner "What Governments Should Do to Respond to Nation State Attacks" Info Security (26 February 2020) Info-Security Group <www.infosecurity-magazine.com>.
- Wolfgang Kleinwächter "International Law and Cyberspace: It's the "How", Stupid" (10 December 2020) CircleID <www.circleid.com>.
- Morten Larsen "While North Korean Missiles Sit in Storage, Their Hackers Go Rampant" (15 March 2021) Foreign Policy <https://foreignpolicy.com>.
- James Lewis "Fighting the Wrong Enemy, aka the Stalemate in Cybersecurity" (26 November 2017) The Cipher Brief <www.thecipherbrief.com>.
- Eliav Lieblich "The Salisbury Incident and the Threshold for "Unlawful Use of Force" under International Law: between Stigmatization and Escalation" (20 April 2018) Stockholm Centre for the Ethics of War and Peace <http://stockholmcentre.org>.
- Neil MacFarquhar "Putin, Responding to Sanctions, Orders U.S. to Cut Diplomatic Staff by 755" (30 July 2017) New York Times <www.nytimes.com>.
- Paul Mee and Til Schuermann "How a Cyber Attack Could Cause the Next Financial Crisis" (14 September 2018) Harvard Business Review <https://hbr.org>.
- Jeff Melnick "Top 10 Most Common Types of Cyber Attacks" (15 May 2018) Netwrix <https://blog.netwrix.com>.
- Nils Melzer "Cyberwarfare and International Law" (02 November 2011) United Nations Institute for Disarmament Research <https://www.unidir.org>.

- Angela Moon "State-sponsored cyberattacks on banks on the rise: report" (23 March 2019) Reuters <www.reuters.com>.
- Harriet Moynihan "The Application of International Law to Cyberspace: Sovereignty and Non-intervention" (13 December 2019) Just Security <www.justsecurity.org>
- Donghui Park and others "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks" (11 October 2017) The Henry M. Jackson School of International Studies: University of Washington <https://jsis.washington.edu>.
- Kim Nash and others "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs" (27 June 2018) Wall Street Journal <www.wsj.com>.
- Lily Newman "The Iran Hacks Cybersecurity Experts Feared May Be Here" (18 December 2018) Wired <www.wired.com>.
- Kari Paul "Russian hackers targeting US political campaigns ahead of election, Microsoft warns" (10 September 2020) The Guardian <www.theguardian.com>.
- Steve Ragan "Stuxnet Likely Constituted Illegal Act of Force, Study Says" (27 March 2013) Security Week <www.securityweek.com>.
- President of the United State, George W Bush "The National Security Strategy of the United States of America" (September 2002) The White House <https://georgewbush-whitehouse.archives.gov>.
- Flavio Paioletti "The 21st Century Challenges to Article 51" (30 June 2021) E-International Relations <www.e-ir.info>.
- Przemyslaw Roguski "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part II" (24 September 2019) Opinio Juris <http://opiniojuris.org>.
- Przemyslaw Roguski "Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace" (03 September 2020) Just Security <www.justsecurity.org>.
- Nicole Perlroth and Quentin Hardy "Banking Hacking Was the Work of Iranians, Officials Say" (08 January 2013) New York Times <www.nytimes.com>.
- David E Sanger and Julian Barnes "The Urgent Search for a Cyber Silver Bullet Against Iran" (23 September 2019) New York Time <www.nytimes.com>.
- David E Sanger "Obama Order Sped Up Wave of Cyberattacks Against Iran" (01 June 2012) New York Times <www.nytimes.com>.
- Sam Sachdeva "NZ's line in the sand on cyberattacks" (07 December 2020) Newsroom <www.newsroom.co.nz>.

- Michael Schmitt and Liis Vihul "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms" (30 June 2017) Just Security <www.justsecurity.org>.
- Michael Schmitt "Germany's Positions on International Law in Cyberspace Part I" (09 March 2021) Just Security <www.justsecurity.org>.
- Michael Schmitt "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis" (14 October 2019) Just Security <www.justsecurity.org>.
- Michael Schmitt and Sean Fahey "WannaCry and the International Law of Cyberspace" (22 December 2017) Just Security <www.justsecurity.org>.
- Michael Schmitt "New Zealand Pushes the Dialogue on International Cyber Law Forward" (08 December 2020) Just Security <https://www.justsecurity.org>.
- Michael Schmitt "Estonia Speaks Out on Key Rules for Cyberspace" (10 June 2019) Just Security <www.justsecurity.org>.
- Thom Shanker and David E Sanger "U.S. Suspects Iran Was Behind a Wave of Cyberattack" (13 October 2012) New York Times <www.nytimes.com>.
- Rebecca Slayton "Why Cyber Operations Do Not Always Favor the Offense" (February 2017) Harvard Kennedy School: Belfer Center for Science and International Affairs <www.belfercenter.org>.
- Catherine Stupp "Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament" (11 June 2020) The Wall Street Journal <www.wjs.com>.
- Emily Tamkin "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" (27 April 2019) Foreign Policy <https://foreignpolicy.com>.
- Federal Government of Germany "On the Application of International Law in Cyberspace" (March 2021) Federal Foreign Office <www.auswaertiges-amt.de>.
- Nicholas Tsagourias "Electoral Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace" (26 August 2019) EJIL: Talk! <www.ejiltalk.org>.
- Ann Väljataga "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly" (2017) CCDCOE <https://ccdcoe.org>.
- James Van de Velde "Cyber espionage is not cyber attack" (21 February) CYISRNET <www.defensenews.com>.
- Christy Un "It's time for the Asia-Pacific to Move toward Regional Cyber Norms" (14 October 2020) The Diplomat <https://thediplomat.com>.

- United States Senate Intelligence Committee "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election" (25 July 2019) U.S. Senate Select Committee on Intelligence <www.intelligence.senate.gov>.
- Joby Warrick and Ellen Nakashima "Officials: Israel linked to a disruptive cyberattack on Iranian port facility" (19 May 2020) The Washington Post <www.washingtonpost.com>.
- Minda Zetlin "Whoever Created the WannaCry Ransomware, Analysis Shows They Speak Chinese" (29 May 2017) INC <www.inc.com>.
- Kim Zetter "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'" (25 March 2013) Wired <www.wired.com>.

D Press Release

- Hillary Rodham Clinton, Secretary of State, Leon Panetta, Secretary of Defense, Kevin Rudd, Minister for Foreign Affairs, and Stephen Smith, Minister for Defence "U.S.-Australia Ministerial Consultations 2011 Joint Statement on Cyberspace" (26th Australia-United States Ministerial Consultations, Washington D.C., 15 September 2011).
- Harold Koh, Legal Adviser of the United States Department of State "International Law in Cyberspace"(USCYBERCOM Inter-Agency Legal Conference on the Roles of Cyber in National Defense, Fort Meade, Maryland, 18 September 2012).
- Aviv Kochavi, Major General of Israel Defense Force "Cyberwar with Iran" (Home Front Command Replacement Ceremony, Tel Aviv, 19 May 2020).

E Interviews

- David Sanger, National Security Correspondent for New York Times (Michael Barbaro, The Daily Podcast, 16 December 2020).

F Speeches:

- Richard Kadlčák, Ministry of Foreign Affairs and Trade for the Cyber Security Department and Special Envoy for Cyber Space, "Special Envoy for Cyberspace Director of Cybersecurity Department of the Open-ended Working Group on

developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations," (United Nations, New York, 11 February 2020)

- Kersti Kaljulaid, President of Estonia, "President of the Republic at the opening of CyCon 2019" (CyCon in Tallinn Estonia, 29 May 2019).
- Miguel Rodríguez, Representative of Cuba "Final Session of Group of Governmental Experts of Developments in the Field of Information and Telecommunication in the Context of International Security" (United Nations, New York, 23 June 2017).
- George W Bush, President of the United States "Pre-emptive military action" (West Point Military Academy graduation, New York, 01 June 2002).