FACULTY OF LAW
Lund University

Demi Bylon

# Jus ad bellum in the 'Wild West'

## Hostile cyber operations and the right to self-defence under international law

LAGF03 Essay in Legal Science

Bachelor Thesis, Master of Laws programme
15 higher education credits

Supervisor: Anders Sjögren

Term: Spring term 2021

# Contents

# Summary

Hostile cyber operations are on the rise and states' critical national infrastructures are facing the threat of being targeted as they become more dependent on computer networks. Cyberspace is persistently referred to as the 'wild West' implicating that the applied international legal framework is insufficient. The international law stipulating jus ad bellum and its applicability to cyber operations in practice is unsettled. In the cyber context, thresholds to a "use of force" in Article 2(4) and an "armed attack" in Article 51 of the UN Charter are vaguely specified and the right to self-defence is disputed.

This thesis aims to examine hostile cyber operations that a state conducts towards another state and jus ad bellum, i.e. under which circumstances a victim state may resort to the use of force. Furthermore, it strives to elucidate the international legal landscape regarding the right to self-defence when a state is subjected to a cyber attack.

The introductory part of the study explains relevant cyber terminology and gives a general overview of jus ad bellum. The main part examines how jus ad bellum applies to cyber operations including threshold assessments and provides a case study of significant cyber attacks as well as state practice.

The final chapter consisting of analysis and concluding thoughts suggest that the steps forward are not proportionate considering the rapidly expanding hostile climate in cyberspace. However, state positions are a welcomed addition to the proceedings of mapping lex lata. The study has shown that the effect-based approach including the criteria scale and effects has been adopted by many states in threshold assessments.  New tendencies in the state practice have also been observed.

# Sammanfattning


Fientliga cyberoperationer ökar och staters kritiska nationella infrastrukturer står inför hotet att bli måltavlor eftersom de i större utsträckning är beroende av datanätverk. Cybersfären benämns ständigt som den ’vilda västern’ vilket antyder att det tillämpade internationella rättsliga ramverket är otillräckligt. Den internationella rätten som föreskriver jus ad bellum och dess tillämplighet på cyberoperationer i praktiken är omstritt. I cybersammanhang är trösklar till ”våldsanvändning” i artikel 2(4) och ”väpnad attack” i artikel 51 i FN-stadgan vagt specificerade och rätten till självförsvar är omtvistad.

Denna uppsats syftar till att undersöka fientliga cyberoperationer som en stat bedriver mot en annan stat och jus ad bellum, det vill säga under vilka omständigheter en attackerad stat kan tillgripa användning av våld. Vidare eftersträvas att belysa det internationella rättsliga landskapet avseende rätten till självförsvar när en stat utsätts för en cyberattack.

Den inledande delen av studien förklarar relevant cyberterminologi samt förser en allmän översikt över jus ad bellum. Huvuddelen undersöker hur jus ad bellum tillämpas på cyberoperationer även inkluderat tröskelbedömningar och ger en fallstudie av betydande cyberattacker samt staters praxis.

Det sista kapitlet som består av analys och avslutande tankar antyder att framstegen inte är proportionerliga med tanke på det snabbt växande fientliga klimatet i cyberssfären. Staters ståndpunkter är dock ett välkommet tillskott till kartläggningen av lex lata. Studien har visat att det effektbaserade tillvägagångssättet inklusive kriterierna skala och effekter har antagits av många stater vid tröskelbedömningar. Nya tendenser i staters praxis har också uppmärksammats.

# Abbreviations

| | |
|---|---|
| CCDCOE | Cooperative Cyber Defence Centre of Excellence |
| CNI | Critical National Infrastructure |
| DDoS | Distributed Denial of Service |
| ICJ | International Court of Justice |
| ICT | Information and Communications Technology |
| NATO | North Atlantic Treaty Organization |
| OEWG | Open-Ended Working Group |
| SCADA | Supervisory Control and Data Acquisition |
| UN | United Nations |
| UNGA | United Nations General Assembly |
| UNGGE | United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security |

# 1 Introduction

## 1.1 Background

In 2015 Barack Obama famously referred to the cyber world as the "wild, wild West"[1] and the United Nations Secretary-General António Guterres used the same rhetoric in his remarks to the UN General Assembly (UNGA) five years later.[2] The cyber sphere is no longer seen as being unregulated since it is settled that international law does apply to cyberspace, however discussions have now shifted to determining the actual application.[3] The persisting reference to the 'wild West' could be interpreted as implications that international law is failing to regulate cyberspace in an appropriate way.

Hostile cyber operations are increasing in numbers and the current pandemic seems to have been exploited for these types of malicious interferences.[4] Imperative functions in society are increasingly dependent on computer networks and the more progressive states are in the technological field, the more vulnerable they will be to fall victim to cyber offences.[5] Between 2017 and 2020 significant nation state cyber attacks increased with 100%[6] and in 2019 there were almost 450 cybersecurity incidents connected to European critical infrastructures, such as finance and energy.[7]

In 2017, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International

---

[1] Obama, Barack, Remarks by the President at the Cybersecurity and Consumer Protection Summit (13 February 2015).
[2] Guterres, António, Remarks to the General Assembly on the Secretary-General's priorities for 2020 (22 January 2020).
[3] Delerue (2020), pp. 1-2.
[4] Schmitt, Texas Nation Security Review (2020), Vol. 3, No. 3, pp. 33-34.
[5] Roscini (2014), p. 1.
[6] McGuire, Michael, Nation states, cyberconflict and the web of profit (2021), p, 4.
[7] European Commission, *Joint communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade* (16 December 2020), p. 3.

Security (UNGGE) failed to reach consensus on the right to self-defence.[8] Consensus is established regarding that cyber operations causing significant damage, destruction, injury or death qualify as unlawful "use of force" in violation of Article 2(4) of the UN Charter and international customary law. However, the criteria for identifying cyber operations as a use of force remain unsettled on the international legal arena. Malicious cyber operations can not only constitute a use of force but also qualify as an "armed attack" in accordance with Article 51 of the UN Charter, which evokes the right to self-defence.[9] In this context, specifying thresholds for hostile cyber operations is of great interest in the legal domain of cyberspace.

## 1.2 Purpose and Research Questions

The purpose of this study will be to examine hostile cyber operations that a state conducts towards another state and jus ad bellum, i.e. under which circumstances a victim state may resort to the use of force. The aim is to elucidate the international legal landscape regarding the right to self-defence when a state is subjected to a cyber attack. To achieve this purpose, the following questions will be answered:

- How does international law regulating jus ad bellum apply to cyber operations?
- Under what circumstances can a cyber attack trigger the right to self-defence?

To answer these questions the relevant cyber terminology and the jus ad bellum regulations will be presented in the following chapters.

[8] Väljataga, Ann, Back to Square one? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly, The NATO CCDCOE, (2017).
[9] Milanovic and Schmitt, Journal of national security, law and policy (2020), Vol. 11. No. 1, pp. 258-259.

## 1.3 Perspective

Since the field of study is discussed and regulated in the context of international law an international perspective will be applied throughout this thesis.

## 1.4 Scope and Delimitations

The scope of this study will be limited to hostile cyber operations conducted by a state towards another state during peacetime and the application of international law. Cyber attacks performed by non-state actors will only be addressed in cases where they may be attributed to a state. Cyber terrorism and cyber crime will therefore not fall within the scope of this thesis. The threat of the use of force, anticipatory and collective self-defence will not be addressed. The main purpose will be to examine cyber operations within the spectrum of jus ad bellum, consequently jus in bello, i.e. international humanitarian law, will not be discussed.

## 1.5 Method and Material

The legal dogmatic method will be used to outline the current legal framework within international law and hence provide answers to the presented research questions.[10] The main focus will therefore be on lex lata, the law as it is, but the analysis will also include elements of lex ferenda, the law as it should be.[11]

The material for this thesis will primarily be evaluated in accordance with Article 38(1) of the Statute of the International Court of Justice regarding sources of international law since it is considered to have general relevance.[12] The sources listed in the article are international conventions, international

[10] Nääv and Zamboni (ed.) (2018), p. 21.
[11] Ibid. p. 36.
[12] Henriksen (2019) p. 23-24 [Henriksen].

custom, recognized general principles, judicial decisions and judicial doctrine.[13] International law does apply to cyberspace, this was disclosed in the consensual reports presented by UNGGE in 2013[14] and 2015[15]. Due to the scarcity of case law and international conventions specifically interpreting and regulating cyberspace, secondary sources will be fundamental for this thesis. The Tallinn Manual 2.0 is the only comprehensive work produced by a wide group of experts in this field and is to be viewed as a secondary source described in Article 38(1)(d).[16] The first edition received criticism for being too Western-focused and therefore the second edition was developed by a more extensive group of experts who also consulted governments during the process.[17]

It should be addressed that the majority of research in English in this field is published by scholars within the Western Hemisphere. Nonetheless, statements from states outside the Western Hemisphere will be presented to provide a broader international perspective.

## 1.6 Previous Research

Legal scholars within the cyber field frequently publish research attempting to sort out grey zones in how international law applies to cyberspace. When it comes to hostile cyber operations and jus ad bellum, novel statements from states and developments in the field make it challenging to settle lex lata. Michael N. Schmitt is a recognized scholar in this field. He writes articles, publishes research and he is the Director of the International Group of Experts who wrote the Tallinn Manual and Tallinn Manual 2.0 sponsored by The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

[13] Art. 38(1), Statute of the International Court of Justice.
[14] UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98, para 19.
[15] UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174, para 24 [2015 UNGGE Report].
[16] Henriksen, p. 32.
[17] Kavanagh (2017), p. 34.

## 1.7 Outline

In order to answer the questions posed this thesis will consist of six chapters. The second chapter will outline the relevant cyber terminology. The third chapter will present jus ad bellum in international law from a general perspective within the scope of the study. The fourth chapter will examine the application of international law regulating jus ad bellum to cyber operations originating from states. The fifth chapter will include a case study of previous cyber attacks and present state practice. The sixth and final chapter will consist of an analysis of the current legal landscape which will then culminate in some final concluding thoughts.

# 2 Cyber Terminology

## 2.1 Cyberspace

The term ‘cyberspace’ was first used by the novelist William Gibson to refer to the total data on all computers on every network in the world. Since then the term has been adopted as a way of referring to any large collection of network-accessible computer-based data.[18] In this thesis the term will be defined as “The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks.”[19]

## 2.2 Cyber operation and cyber attack

‘Cyber operation’ will be a fundamental term in this thesis and will be defined as ‘The employment of cyber capabilities to achieve objectives in or through cyberspace.’[20] The term ‘cyber attack’ is oftentimes used in reference to any kind of hostile operation directed at cyber infrastructure, services, applications or users. No universal definition exists, and many nation states have their own definition in their cyber security strategies. For the purpose of this thesis the definition will be of a more legal character. ‘Cyber attack’ will constitute a cyber operation that could qualify as prohibited use of force under Article 2(4) and also amount to the threshold of an ‘armed attack’ under Article 51 in the UN Charter.[21]

## 2.3 Types of cyber operations

Critical National Infrastructure (CNI), such as financial institutions, electric power, telecommunications and transportation are becoming recurrent targets to malicious cyber operations while progressively becoming more dependent

[18] A Dictionary of Computer Science (7 ed.) (2016), p. 66.
[19] Schmitt and Vihul (ed.) (2017) p. 564 [Tallinn Manual 2.0].
[20] Ibid.
[21] Ericson (2020), pp. 38-39 [Ericson].

on information systems.[22] Most commonly used in hostile cyber operations is ‘malware’[23], i.e. software that is designed to affect the performance of a computer system. The malware can be in the form of Trojan horses, rootkits, viruses, and worms. ‘Distributed Denial of Service’ (DDoS) is another technique that employs multiple computing devices to cause ‘denial of service’ (DoS) which translates to denying the availability of computer system resources to their users. DDoS can employ a ‘botnet’, i.e. a network of compromised computers, so-called ‘bots’ remotely controlled by an intruder used to conduct coordinated cyber operations.[24] A more recently emerging type of cyber operation is the so-called ‘ransomware attack’ where the targeted data gets encrypted and the owner has to make a payment for it to be decrypted.[25]

[22] Maogoto (2015), p. 1.
[23] Ibid. p. 58.
[24] Tallinn Manual 2.0, pp. 563-566.
[25] Ericson, pp. 21-23.

# 3 Jus ad bellum

Jus ad bellum constitutes the law that regulates when and for what purpose a state may use force against another state.[26]

## 3.1 The prohibition of the use of force

Article 2(4) in the UN Charter discloses the prohibition of the use of force:

> *All member states 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.*[27]

The prohibition is established in customary international law since the International Court of Justice (ICJ) settled the *Nicaragua Case* in 1986.[28] Even if an interference is not assessed to be in violation of Article 2(4) it can still be an unlawful act under international law.[29]

## 3.2 The right to self-defence

Article 51 in the UN Charter stipulates an exception to the prohibition of the use of force in Article 2(4):

> *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 under the present Charter to take at any time such action*

[26] Henriksen, p. 254.
[27] Art. 2(4), Charter of the United Nations.
[28] *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States*), Merits (1986) ICJ Rep 14, para. 174 [*Nicaragua*].
[29] Henriksen, p. 257.

*as it deems necessary in order to maintain or restore international peace and security*.[30]

In like manner, ICJ stated that the right to self-defence constitutes customary international law in *Nicaragua*.[31] In order to validate a victim state's self-defence the interference has to qualify as an armed attack. The attack must be of a certain intensity – only acts that are probable to cause severe damages like territorial invasion, human casualties or massive destruction of property will qualify.[32] In the *Nuclear Weapons Case*, the ICJ stated that articles on the use of force "apply to any use of force, regardless of the weapons employed". [33] The accumulation of events doctrine, i.e. where the severity of a series of hostile acts is assessed cumulatively, has been under discussion but gained support over time.[34]

Self-defence has to be initiated during the armed attack or not too long after the attack ceased. In addition, self-defence has to be necessary and proportionate. The victim state is able to exercise self-defence as a last resort and the force used should only be of the extent needed to terminate the attack. If force of a higher degree is needed the UN Security Council have to grant it through authorization in accordance with Chapter VII of the UN Charter.[35]

30 Art. 51, Charter of the United Nations.
31 *Nicaragua* (n 13) paras. 193 and 176.
32 Henriksen, p. 267.
33 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion (1996) ICJ Rep 226, paras 38-39 [*Nuclear Weapons*].
34 Henriksen, p. 267.
35 Ibid. pp. 270-271.

# 4 Application of the jus ad bellum regime to cyber operations

In 1945 when the UN Charter came about only kinetic force, i.e. physical conventional warfare, was thought of when putting the use of force regime into place.[36] However, ICJ settled that the "weapons employed" is not a factor that determines the regulation's applicability.[37] The prohibition of the use of force applies to any use of force, including non-kinetic force such as cyber operations.[38] In addition, it is commonly accepted that international law applies to cyberspace as stated in the 2015 UNGGE report[39] which got endorsed by the UN General Assembly.[40]

## 4.1 Imperative thresholds

**Use of force**

In order for Article 2(4) and its customary equivalent to be applicable to cyber operations it has to be attributed to a state. In addition, it has to amount to the threshold of the use of force and it has to be conducted towards another state.[41] However, there is no general definition presented in the UN Charter regarding what the term 'force' includes. The prevailing view is that the scope is limited to 'armed force' and therefore does not include economical, ideological or political coercion.[42] The aim is to identify the threshold between an intervention and a use of force. In order for an intervention to amount to armed force it has to rise to a certain level of severity through military means in a state-to-state situation. The intervention can be carried out directly, or

---

36 Maogoto (2015), p. 4.
37 *Nuclear Weapons*, para 39.
38 Tallinn Manual 2.0, p. 328.
39 2015 UNGGE Report, p 12.
40 UNGA, "Developments in the field of information and telecommunications", Resolution 70/237, 23 December 2015.
41 Roscini, 'Cyber operations as a use of force', in Tsagourias and Buchan (2015), pp. 233-235.
42 Tallinn manual 2.0, p. 331; Ericson, pp. 211-213.

indirectly (e.g. employing guerrillas in favour of another state).[43] In the cyber context, an effect-based approach has been adopted predominantly to distinguish a use of force.[44] The Tallinn Manual 2.0 refers to the practice of assessing "scale and effects" of an operation on the basis of the *Nicaragua Case*[45]. ICJ used this approach when determining if certain acts had crossed the threshold to an armed attack and it is claimed to be as effective in the assessment of the use of force.[46] However, there are scholars that advocate for applying the effect-based approach together with the target-based approach which focuses on the target of the cyber attack and its importance for the victim state. The instrument-based approach has been rejected by scholars since its focal point is whether the cyber attack can be seen as a weapon that could exercise armed force.[47]

A clear case of a hostile cyber operation constituting a use of force is when it causes human casualties or physical damage to property.[48] Additionally, all operations rising to the level of an armed attack and that can be attributable to a state are uses of force.[49] For the cyber operations that are more challenging to evaluate, factors to take into account are presented in the Tallinn Manual 2.0. The aim is to provide guidance and simplify the analogy to acts that the majority of states would qualify as a use of force. The factors are severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality. Depending on the case, more factors can be taken into account and the list is therefore not exhaustive.[50]

Even if a cyber operation does not qualify as a use of force, it can still be unlawful by either constituting a violation of sovereignty or a breach of the

[43] Ericson, pp. 214-215.
[44] Ibid. p. 219.
[45] *Nicaragua*, para 195.
[46] Tallinn Manual 2.0, pp. 330-331.
[47] Focarelli, 'Self-defence in cyberspace', in Tsagourias and Buchan (2015), p. 265; Ericson, p. 219.
[48] Roscini (2014), p. 53.
[49] Tallinn Manual 2.0, p. 332.
[50] Ibid. pp. 333-337.

prohibition of intervention.[51] Furthermore, a state being subject to a use of force that does not rise to the level of an armed attack cannot lawfully practice self-defence, but could instead have mandate to use countermeasures or actions in line with the plea of necessity.[52]

**Armed attack**

Besides the threshold addressed above, there is an additional threshold for the most severe forms of use of force, constituting an 'armed attack' referred to in Article 51 of the UN Charter.[53] As with the case of the use of force, there is no definition of the term 'armed attack' in the UN Charter.[54] Fundamentally, to constitute an armed attack and thereby justify self-defence the cyber attack has to qualify as a use of force in accordance with Article 2(4).[55] The International Group of Experts unanimously affirms the view that a hostile cyber operation may amount to the level of severity that is required to qualify as an armed attack. This view is in alignment with the position expressed from states. An act of 'aggression', as defined by the UN General Assembly[56], can be classified as an armed attack in some cases.[57] However, it is expressed in the Tallinn Manual 2.0 that the term aggression in itself does not target the right to self-defence.[58]

In *Nicaragua*, ICJ stated that armed attacks must be separated as "the gravest forms of the use of force […] from other less grave forms". [59] An armed attack must amount to certain "scale and effects",[60] and therefore, in order for a cyber attack to be classified as an armed attack it has to be characterized as 'grave' on the spectrum of the use of force. Collection of cyber intelligence and cyber operations that disrupt non-crucial functions exemplify acts which

[51] Tallinn Manual 2.0, p. 330.
[52] Ibid. p. 337.
[53] Ericson, pp. 216-217.
[54] *Nicaragua*, para. 176.
[55] Focarelli, 'Self-defence in cyberspace', in Tsagourias and Buchan (2015), p. 256.
[56] Declaration on the Definition of Aggression, GA Resolution 3314 (XXIX), 14 December 1974.
[57] Roscini (2014), p. 71.
[58] Tallinn Manual 2.0, p. 339.
[59] *Nicaragua*, para. 191.
[60] Ibid.

do not amount to an armed attack. Nevertheless, acts that cause serious human casualties or 'significant' physical damage to property qualify as an armed attack. The International Group of Experts holds the view that the accumulation of effects doctrine could apply to cyber operations, meaning that several interferences of smaller scale could rise to the level of an armed attack collectively.[61]

Further specification of the threshold continues to be vague. Certain hypothetical scenarios are debated amongst scholars, e.g. if a cyber attack would cause an international stock market to crash. Some argue that the financial aspect eliminates the possibility to qualifying such acts as an armed attack, meanwhile some argue that such functions are associated with CNI and therefore could amount to the threshold.[62]

There have been discussions regarding if data could be seen as property in the modern society which then could make a destruction of data amount to the use of force in Article 2(4) and further constitute an armed attack. This broad interpretation of Article 2(4) has not gained acceptance in the international community. These types of cyber operations could instead be a violation of the principle of non-intervention.[63]

**Necessity and proportionality**

Once the right to self-defence is triggered, the self-defence can be either kinetic, electronic or be of cyber character. [64] In order to be lawful the acts in self-defence have to be necessary and proportionate. These principles have been established as customary international law through being referred to in *Nicaragua*[65] and the *Oil Platforms Case*.[66]

---

[61] Tallinn Manual 2.0, pp. 341-342.
[62] Ibid. pp. 342-343.
[63] Roscini, 'Cyber operations as a use of force', in Tsagourias and Buchan (2015), pp. 244-245.
[64] Roscini (2014), p. 69.
[65] *Nicaragua*, para. 176.
[66] *Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America*), Judgment, 6 November 2003, ICJ Rep 2003, paras. 43, 73-74, 76; Tallinn Manual 2.0 p. 348.

The principle of necessity entails that the use of force is exercised by the victim state as a last resort to withstand the imminent armed attack. The victim state can deter the attack by other means but responding with force in self-defence demands that other measures are deemed to be inadequate from the victim state's perspective (e.g. firewalls). A combination of such measures can also be a lawful alternative.[67] This can be interpreted as states having to account for implementing cyber defensives to be able to assess that they are insufficient.[68]

The principle of proportionality corresponds to the legitimacy of the level of force employed. The kinetic or cyber self-defence has to be reasonable assessed after its scope, duration and intensity.[69] Immediacy in regards of self-defence in the cyber sphere is also of importance. However, cyber incidents can be difficult to evaluate rapidly since the effects of a malicious cyber operation can be delayed and the identification of the originator can be time-consuming. Thus, the International Group of Experts concludes that the criterion of immediacy is met as long as it is deemed reasonable for the victim state to respond.[70]

## 4.2 The complexity of attribution

To determine the origin of a cyber operation is a challenging occupation and failing to do so could hinder the application of Article 2(4).[71] A hostile cyber operation has to be attributed to a state in order to constitute a use of force in accordance with the article.[72] This matter is also of essence in the following

[67] Tallinn Manual 2.0, pp. 348-349.
[68] Focarelli, 'Self-defence in cyberspace', in Tsagourias and Buchan (2015), p. 275.
[69] Tallinn Manual 2.0, p. 349.
[70] Ibid. pp. 353-354.
[71] Roscini, 'Cyber operations as a use of force', in Tsagourias and Buchan (2015), p. 234.
[72] Ericson, p. 211.

stage of determining if an act of self-defence could be lawful under international law.[73]

In the Tallinn Manual 2.0, the International Group of Experts applies The International Law Commission's Articles on State Responsibility[74] which is commonly recognized as a reflection of customary international law.[75] Rule 15 states that:

*Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State.*[76]

'Organs of a State' should be broadly interpreted and encompass any person or entity that holds an official status in the domestic law of the state.[77] A state can be subject of attribution if it has instructed or practiced effective control over a non-state actor that carried out a hostile cyber operation towards another state.[78] Specific cyber strategies, such as making evidence point to false originators by impersonating IP-addresses, are also addressed.[79]

It is encouraged that states provide substantiation for allegations of hostile cyber operations; however, it has been rare to actually do so. States have argued that there should be no legal obligation to present evidence due to such material potentially compromising details of cyber technology and strategies. To present a convincing case of attribution without substantiation can be challenging,[80] yet victim states are becoming more prone to voice attribution.[81] States such as the UK, Australia and Canada has attributed

[73] Tallinn Manual 2.0, p. 344.
[74] Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the International Law Commission, vol. II, Part Two, 2001.
[75] Henriksen, p. 121.
[76] Tallinn Manual 2.0, p. 87.
[77] Ibid.
[78] Shany, Yuval and Schmitt, Michael N., An International Attribution Mechanism for Hostile Cyber Operations, 96 Int'l L. Stud. 196 (2020), p. 199.
[79] Tallinn Manual 2.0, p. 92.
[80] Shany, Yuval and Schmitt, Michael N. (2020), p. 213.
[81] Ibid. p. 211.

cyber operations and the US proceeded with pressing charges against North Korean and Russian citizens who allegedly were involved in attacks. Some states have declared that attribution is a sovereign judgment and states can therefore make public statements if they wish.[82] In the same manner, EU's Cyber Diplomacy Toolbox states that attribution is a "sovereign political decision" which should correspond to the international law of state responsibility.[83]

The complex endeavour to identify the originator of hostile acts is not only faced in the cyber sphere, but also in the legal sphere of international terrorism. Hence the complexity should not be used as an excuse to neglect legal measures.[84] As a way forward, scholars have suggested that an independent attribution mechanism could be a way of improving the uncertainty of attribution.[85]

## 4.3 Group of Governmental Experts and the Open-ended working group

UNGGE and OEWG are important forums where states can negotiate norms, rules and principles applicable to ICTs. The worsening threat environment in cyberspace might have the positive effect of pressuring states to reach consensus agreements.[86]

**Group of Governmental Experts**

The UNGGE's aim is to create a foundation of recommendations by reaching consensus regarding how international law applies to ICTs. As previously mentioned, the reports from 2013 and 2015 were successfully presented while

---

[82] Ericson, pp. 111-112.
[83] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 9916/17, 7 June 2017.
[84] Roscini (2014), p. 33.
[85] Shany, Yuval and Schmitt, Michael N. (2020), pp. 221-222.
[86] UNIDIR, Cyber Stability Conference 2019: Strengthening Global Engagement, New York, 6 June 2019, p. 3.

positions seemed to have been too far apart in 2017, resulting in the absence of a report.[87] The US took initiative suggesting a new UNGGE in 2018 and the report is scheduled to be presented during 2021.[88]

**Open-ended working group**

In 2018 the Russian Federation handed in a resolution which would result in the establishment of the OEWG in parallel with the UNGGE. This group is more inclusive since any of the 193 UN Member states can partake in contrast to the UNGGE who consists of a smaller group of experts. In March 2021 the group's first consensus report was approved and in the Chair's Summary there were noteworthy requests for clarification concerning the thresholds of the 'use of force' and 'armed attack'.[89]

[87] Ericson, pp. 112-113.
[88] Ibid. pp. 113-114.
[89] UNGA, 'Chair's Summary of the Open-ended working group on developments in the field of information and telecommunications in the context of international security' (10 March 2021), UN Doc. A/AC.290. para. 18.

# 5 Case study and state practice

## 5.1 Case study

The following cases will shed light on cyber attacks that have been addressed extensively by scholars within the field and give example to threshold judgments in practice.

### 5.1.1 Estonia

In 2007, Estonia fell victim to extensive cyber attacks targeting CNI including the banking system, government functions and the media. The DDoS-attacks created an overflow of information requests which made systems shut down for several weeks. At the time, Estonia was one of the most networked societies in Europe and was a frontrunner in digitalizing government services. It has been implied that Russia was responsible for the attack, but this was later denied and there is not enough evidence to prove attribution. Estonian government officials thought that NATO should have responded in accordance with Article 5 in the North Atlantic Treaty stating collective self-defence, but their claim was dismissed.[90]

The majority of scholars agree that this case did not amount to a use of force. This conclusion is based on timespan, the severity of the disruptions and that no physical property or people suffered any casualty. It is argued that these attacks, due to not reaching the threshold of a use of force, constitute prohibited interventions. However, it has been articulated that this sort of cyber attacks could constitute a use of force in the future. With the world becoming more digitalized by the day, the assessment of severity can shift in conjunction with higher dependency in digital financial services.[91]

[90] Focarelli, 'Self-defence in cyberspace', in Tsagourias and Buchan (2015), pp. 259-260.
[91] Ericson, pp. 238-240.

### 5.1.2 Stuxnet

Between June 2009 and May 2010[92], malware in form of a worm attacked the industrial supervisory control and data acquisition (SCADA) system in an Iranian nuclear facility. The worm was named "Stuxnet" and is the first known worm created to target infrastructure outside of the cyber sphere – it was created to launch a cyber attack that would destroy an industrial process in the physical world. Stuxnet affected the velocity of centrifuges that enrich uranium which is an imperative element in nuclear facilities. Due to the effectiveness of the worm to infiltrate an ultra-secure facility it is believed to have attribution to governmental agents.[93] It has been claimed that the US and Israel were responsible for the Stuxnet attack, but no conclusive evidence has been presented to support the claim.[94]

This was the first cyber attack that caused kinetic effects, resulting in centrifuges in the nuclear facility shutting down. If attribution could be determined, then the attack could qualify as an armed attack under international law.[95] It constituted a use of force, but it is disputable whether its scale and effects rose to the level of an armed attack.[96]

## 5.2 State practice

Various states ascribe cyberspace to be the fifth domain of warfare, incorporate cyber technologies in their military doctrines and employ specialized cyber units.[97] However, since state practice within the cyber sphere customarily is classified it is difficult to trace opinio juris.[98] States have also been reluctant to verbally express their stance in the legal debate.[99] Nevertheless, states will continue to have the key role in bringing clarity as

[92] Roscini (2014), p. 6.
[93] Maogoto (2015), pp. 53-54.
[94] Focarelli, 'Self-defence in cyberspace', in Tsagourias and Buchan (2015), p. 261.
[95] Ericson, p. 25.
[96] Delerue (2020), p. 341.
[97] Roscini, 'Cyber operations as a use of force', in Tsagourias and Buchan (2015), p. 239.
[98] Tallinn Manual 2.0, p. 3.
[99] Schmitt, Michael N. (2020), p. 36.

to how international law applies to cyberspace and existing statements represent trends in different regions.[100] The following exposition does not set out to be exhaustive, but it includes a majority of public positions.

### China

In China's submission to the OEWG it is expressed that the principle of the prohibition of the use of force is applicable to cyberspace. No views on thresholds are disclosed, instead it is emphasized that conflicts amongst states should be solved in a peaceful course of action. Jus ad bellum and its applicability should be managed with caution and China is in favour of developing new legal instruments adapted to ICTs.[101]

### The Russian Federation

During the 2017 UNGGE Russia, China and Cuba were among the states that expressed strong opposition to the discussion on the right to self-defence. Andrey Krutskikh, representing the Russian Foreign Ministry, expressed that the use of force regime is inappropriate to apply to cyberspace and real space. Technical and legal measures of attribution should be consulted before resorting to self-defence and ICTs should be used peacefully.[102] Cyberspace should not emerge as a novel battlefield[103] and Russia have expressed the will to develop international law instruments regulating ICTs.[104]

### Israel

Israel agrees that hostile cyber operations can constitute a use of force and if the attack is 'imminent' then it could also trigger the right to self-defence. Kinetic or cyber self-defence may be exercised if it is deemed necessary and

---

[100] Schmitt, Michael N. (2020), pp. 36-38.
[101] China, China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2020), p. 6.
[102] Väljataga, Ana (2017).
[103] Ericson, p. 115.
[104] Henderson, 'The United Nations and the regulation of cyber-security', in Tsagourias and Buchan (2015), p. 468.

proportionate. Israel expressed that it is yet to review whether operations could qualify as a use of force even in the absence of physical damage.[105]

**European Countries**

When it comes to the prohibition of the use of force Germany agrees with the Tallinn Manual 2.0 regarding that malicious cyber operations should be assessed by its ‘scale and effects’. If the cyber operation would amount to the damage of a conventional kinetic use of force, then it would qualify as such. The assessments are to be conducted in a case-to-case approach and qualitative criteria have to be taken into account.[106]

Regarding the right to self-defence, Germany’s view corresponds with what is presented in the Tallinn Manual 2.0. It is also expressed that if the threshold to the right to self-defence is crossed, then the victim state can use any measures needed to end the hostile cyber operation as long as they are necessary and proportionate.[107] Overall, this view is shared by the Netherlands,[108] Finland[109] and France. However, France view is that a cyber operation that causes “substantial loss of life or considerable physical or economic damage” can qualify as an armed attack.[110] The Netherlands has also expressed that “at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force.”[111]

[105] Israel, Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (2021) pp. 398-399.
[106] Germany, On the Application of International Law in Cyberspace, Position paper (2020), p. 4.
[107] Ibid. p. 15.
[108] The Netherlands, Appendix: International law in cyberspace (2019), p. 8.
[109] Finland, International law and cyberspace Finland’s national positions (2020), p. 6.
[110] France, International Law Applicable to Operations in Cyberspace (2019), pp. 6-8.
[111] The Netherlands, Appendix: International law in cyberspace (2019), p. 4.

**The US, Australia, New Zeeland, the UK and Canada (so-called "Five-Eyes")**

The US holds the view that self-defence can be used if a hostile cyber operation qualifies as an "actual or imminent armed attack".[112] In 2012, it was addressed by Harold Koh that the US holds the position that there is no threshold between a prohibited use of force and an armed attack. However, the response in self-defence needs to be necessary and proportionate.[113] The US's International Strategy for Cyberspace from 2011 declares that "when warranted, the Unites States will respond to hostile acts in cyber space as we would to any other threat to our country".[114]

The UK's previous Attorney General declared that the prohibition of the use of force applies to cyberspace and that states have the right to resort to self-defence when a cyber operation amount to the severity of an armed attack.[115] New Zeeland adopts the 'scale and effects' approach when it comes to the use of force and the threshold for an armed attack.[116] In like manner Australia cites 'scale and effects' in its position annex[117] and Canada has not yet clarified its stance.[118]

**NATO**

NATO's AJP-3.20 doctrine adopts 'scale and effects' as criteria to consider in threshold assessments for the use of force and for an armed attack. The member states further agree with the position that a case-to-case approach has to be employed. The document was approved by all 30 member states.[119]

---

[112] Brian J. Egan, International Law and Stability in Cyberspace, 35 Berkeley J. Int'l Law. 169 (2017). pp. 177-178.
[113] Koh, H.H., Legal Adviser of the US State Dep't, Remarks at the US Cyber Command Inter- Agency Legal Conference (18 September 2012).
[114] The United States, International Strategy for Cyberspace (May 2011), p. 14.
[115] Wright, J, Attorney General, Remarks at Chatham Royal Institute for International Affairs, 'Cyber and International Law in the 21st Century' (23 May 2018).
[116] New Zeeland, The Application of International Law to State Activity in Cyberspace (2020), paras. 6-8.
[117] Australia, Annex B: Australia's position on how international law applies to State conduct in cyberspace (2020), para. 1.
[118] Gold, Josh, Parson, Christopher and Poetranto, Irene, 'Canada's Scattered and Uncoordinated Cyber Foreign Policy: A Call for Clarity' (2020).
[119] NATO, Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations (2020), p. 20.

# 6 Analysis and conclusion

Undoubtedly, the research questions examined in this study have been asked by states, practitioners and scholars for many years. A number of factors makes these legal discussions more pressing by the day, such as states CNIs to a vast extent are dependent on ICTs for fundamental functioning. Cyber interferences are on the rise and working groups such as the UNGGE and OEWG are contributing to a progression in the right direction, but the steps forward are not proportionate considering the rapidly expanding hostile climate in cyberspace. The vague outcomes and takeaways from these processes have made states and state member organizations present their positions on interpretation of international law applied to hostile cyber operations. Although these positions seem to differ in some respects, it is a welcomed addition to the proceedings of mapping lex lata.

*How does international law regulating jus ad bellum apply to cyber operations?*

Even if China and Russia have emphasized a preference for developing an international legal instrument regulating ICTs it is well established that international law applies to cyberspace. China and Russia have further expressed a dissatisfaction with discussing the jus ad bellum regime in the context of cyber operations. The absence of the UNGGE report in 2017 gives an example of this since the right to self-defence was one of the principal watersheds. However, the opposite view where analogy is used to navigate the legal landscape seems to be the prevailing one considering the newly presented state positions and the Tallinn Manual 2.0 having a broader participation of experts. Russia’s initiative to the more inclusive OEWG also showcases a will to reach agreement beyond the Western Hemisphere.

Article 2(4) of the UN Charter is applicable to a cyber operation if it is attributed to a state and constitute a use of force. To distinguish a cyber intervention from a cyber use of force the effect-based approach is the most endorsed one by scholars and states. Criteria such as scale and effects should be consulted as cited in the Tallinn Manual 2.0 and more frequently referred to in position documents. These criteria can also be used when conducting an 'armed attack' threshold assessment. The consensus regarding that a cyber operation that causes significant damage, destruction, injury or death would qualify as unlawful use of force under Article 2(4) is unsatisfactory. As the case study shows, cyber attacks can cause extensive harm and not only is attribution an obstacle, but threshold assessment appears to be rigid. The analogies have to be more adaptable and precise in order for the law to be effective in its application to cyber attacks. The factors presented in the Tallinn Manual 2.0 to aid analogy in the case-to-case approach is adequate guidance.[120]

In order for a cyber attack to amount to an armed attack and trigger the right to self-defence it has to constitute a grave use of force. Its scale and effects have to reach a certain severity. Cyber operations that disrupts non-crucial functions does not meet the threshold, while acts that causes serious human casualties or 'significant' physical damage to property qualify. The accumulation of effects doctrine could also apply which would be preferable considering the characteristics of certain cyber attacks, e.g. DDoS. Cyber attacks that would cause financial damage are not yet accepted as interference that could qualify as a use of force and an armed attack, but it seems like there are indications from states and scholars that this could gain more support in the future. France and the Netherlands have already expressed that such effects could qualify. Additionally, it is accepted that once the right to self-defence is triggered the victim state can respond with either kinetic or cyber means as long as they are necessary and proportionate. Self-defence is to be used as a last resort and should be conducted within the frames of immediacy.

[120] See section 4.1.

In the process of determining attribution the International Law Commission's Articles on State Responsibility are to be consulted. However, the nature of cyber attacks complicates attribution and the current procedure can hinder states from resorting to lawful self-defence. Therefore, the development of new attribution strategies should be encouraged.

*Under what circumstances can a cyber attack trigger the right to self-defence?*

Highlighting what is stated above, the cyber attack has to constitute a grave use of force amounting to the severity of an armed attack in accordance with Article 51 of the UN Charter in order to trigger the right to self-defence. The attack must have significant scale and effects and substantiation for attribution to a state should be presented, or at least be determined. Acts that causes serious human casualties or 'significant' physical damage to property are frequently referred to as clear cases. It is unsettled whether financial damage can trigger the right to self-defence, yet the accumulation of effects doctrine may be lawful to apply.

**Concluding thoughts**

This thesis has shown that the effect-based approach including the criteria scale and effects have been adopted by many states. Even if there are polarization between states, mainly showcased by Russia, China and the US, a clear trend in states positions can be detected. NATO's AJP-3.20 doctrine which was approved by all 30 member states is a significant contribution. Tendencies towards assessing attacks with the same characteristics as Estonia, such as financial damage, are noteworthy.

The unfolding of positionings from additional states and outcomes from the processes of UNGGE and OEWG will be crucial contributions to the legal regulation of cyberspace and hopefully, once and for all, eliminate references to the 'wild West'.

# Bibliography

## Literature

Delerue, Francois, *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020.

Ericson, Marika, *On the virtual borderline: cyber operations and their impact on the paradigms for peace and war: aspects of international and Swedish domestic law*, Uppsala universitet, Diss. Uppsala: Uppsala universitet, 2020, Uppsala, 2020.

Henriksen, Anders, *International law*, Second edition, Oxford University Press, Oxford, 2019.

Maogoto, Jackson Nyamuya, *Technology and the law on the use of force: new security challenges in the twenty first century*, Routledge, Oxfordshire, England, 2015.

Nääv, Maria and Zamboni, Mauro (red.*), Juridisk metodlära*, Second edition, Studentlitteratur, Lund, 2018.

Tsagourias, Nikolaos and Buchan, Russell (red.), *Research handbook on international law and cyberspace*, Edward Elgar Publishing, Cheltenham, 2015.

Roscini, Marco, *Cyber operations and the use of force in international law*, Oxford University Press, Oxford, 2014.

Schmitt, Michael N. and Vihul, Liis (red.), *Tallinn manual 2.0 on the international law applicable to cyber operations: prepared by the international group of experts at the invitation of the NATO cooperative* *cyber defence centre of excellence*, Second edition., Cambridge University Press, Cambridge, United Kingdom, 2017 [Tallinn Manual 2.0].

## International Treaties and Conventions

United Nations, *Charter of the United Nations*, 24 October 1945.

United Nations, *Statute of the International Court of Justice*, 18 April 1946.

## Table of cases

### International Court of Justice

*Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States),* Merits, Judgment of 27 June 1986, ICJ Reports 1986.

*Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment, 6 November 2003, ICJ Reports 2003.

*Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, ICJ Reports 1996.

## Journals

Milanovic, Marko and Schmitt, Michael N., 'Cyber Attacks and Cyber (Mis)information Operations During a Pandemic', Journal of national security, law and policy (2020), Vol. 11. No. 1.

Schmitt, Michael N., 'Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace', Texas Nation Security Review (2020), Vol. 3, No. 3.

Shany, Yuval, Schmitt, Michael N., 'An International Attribution Mechanism for Hostile Cyber Operations', International Law Studies (2020), 96 Int'l L. Stud. 196.

## Official Documents

Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries, *Yearbook of the International Law Commission*, vol. II, Part Two, 2001.

European Commission, *Joint communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 final, Brussels, 16 December 2020.

General Secretariat of the Council, Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") Adoption, 9916/17, 7 June 2017.

## Resolutions

UN General Assembly Resolution 3314 (XXIX), 'Definition of Aggression', UN Doc. A/RES/29/3314, 14 December 1974.

UN General Assembly, 'Developments in the field of information and telecommunications', Resolution 70/237, 23 December 2015.

## Reports

Kavanagh, Camino, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century,* UNIDIR, 2017.

UNIDIR, *Cyber Stability Conference 2019: Strengthening Global Engagement*, New York, 6 June 2019.

UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013), UN Doc. A/68//98.

UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015), UN Doc. A/70/174.

UNGA, 'Chair's Summary of the Open-ended working group on developments in the field of information and telecommunications in the context of international security' (10 March 2021), UN Doc. A/AC.290/2021/CRP.3.

## Internet sources

### Statements from states and organizations

Australia, Annex B: Australia's position on how international law applies to State conduct in cyberspace (2020), <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>, accessed 12 May 2021.

Brian J. Egan, International Law and Stability in Cyberspace, 35 Berkeley J. Int'l Law. 169 (2017), <https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf>, accessed 4 May 2021.

China, China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2020), <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf>, accessed 6 May 2021.

Finland, International law and cyberspace Finland's national positions (2020), <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727>, accessed 6 May 2021.

France, International Law Applicable to Operations in Cyberspace (2019), <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf>, accessed 5 May 2021.

Germany, On the Application of International Law in Cyberspace, Position paper (2021), <https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf>, accessed 3 May 2021.

Israel, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 97 INT'L L. STUD (2021), <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2957&context=ils>, accessed 12 May 2021.

Koh, H.H., Legal Adviser of the US State Dep't, Remarks at the US Cyber Command Inter-Agency Legal Conference (18 September 2012), <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>, accessed 3 May 2021.

NATO, Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations (2020), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf>, accessed 5 May 2021.

New Zeeland, The Application of International Law to State Activity in Cyberspace (2020), <https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf>, accessed 6 May 2021.

The Netherlands, Appendix: International law in cyberspace (2019), <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>, accessed 7 May 2021.

The United States, International Strategy for Cyberspace (May 2011), <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>, accessed 3 May 2021.

Wright, J, Attorney General, Remarks at Chatham Royal Institute for International Affairs, ”Cyber and International Law in the 21st Century”, May 23, 2018 (15 September 2018), <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, accessed 3 May 2021.

### Other sources

A Dictionary of Computer Science (ed. Butterfield & Ngondi), 7th edition, Oxford University Press, online version published 2016, <https://www.oxfordreference.com/view/10.1093/acref/9780199688975.001.0001/acref-9780199688975>, accessed 12 April 2021.

Gold, Josh, Parson, Christopher and Poetranto, Irene, Canada’s Scattered and Uncoordinated Cyber Foreign Policy: A Call for Clarity, Just Security (4 August 2020), <https://www.justsecurity.org/71817/canadas-scattered-and-uncoordinated-cyber-foreign-policy-a-call-for-clarity/>, accessed 6 May 2021.

Guterres, António, Remarks to the General Assembly on the Secretary-General's priorities for 2020 (22 January 2020), <https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020>, accessed 18 April 2021.

McGuire, Michael, Nation States, Cyberconflict and the Web of Profit, Threat Research HP Inc., (2021), < https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf>, accessed 16 April 2021.

Obama, Barack, Remarks by the President at the Cybersecurity and Consumer Protection Summit (13 February 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>, accessed 4 April 2021.

Väljataga, Ann, 'Back to Square one? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly', The NATO CCDCOE, (1 September 2017), <https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/>, accessed 12 May 2021.