Anna Teirfolk

INTERNATIONALLY WRONGFUL ACTS IN CYBERSPACE: ALLOCATING STATE RESPONSIBILITY FOR "BELOW THE THRESHOLD" CYBER OPERATIONS

Master's Thesis in Public International Law

Supervisor: Mikaela Heikkilä

Faculty of Social Sciences, Business and Economics

Åbo Akademi University

2020

ÅBO AKADEMI – FACULTY OF SOCIAL SCIENCES, BUSINESS AND ECONOMICS
Abstract for Master's Thesis

Subject: Public International Law	
Author: Anna Teirfolk	
Title of the Thesis: Internationally Wrongful Acts in Cyberspace: Allocating State Responsibility for "Below the Threshold" Cyber Operations	
Supervisor: Mikaela Heikkilä	

State cyber operations that occur during peacetime and fall below the threshold of prohibited uses of force have become commonplace. Over the past decade, it has been estimated that over a hundred states have acquired the technological capabilities to launch cyber operations against other states, causing damage to critical infrastructure, official databases, or governmental computer systems. Approximately thirty states have been accused of having conducted or supported such malicious cyber activity, a recent example being a series of alleged Russian cyber operations targeting organizations in Canada, the U.K., and the U.S. involved in the development and testing of potential COVID-19 vaccines. Moreover, since the beginning of the novel coronavirus pandemic, the World Health Organization (WHO) has reported a fivefold increase in cyber operations conducted against hospitals and other medical facilities around the world.

In the absence of a cyber-specific treaty, the applicability of international law to cyberspace is widely dependent on customary international law. Therefore, by applying existing customary rules of state responsibility, the thesis examines how cyber operations may constitute internationally wrongful acts by violating state sovereignty and the principle on non-intervention into the internal or external affairs of another state.

For state responsibility to arise, the conduct must be unlawful and attributable to a state. The majority of the official state positions and national cyber security strategies examined in the thesis affirm that state sovereignty is applicable in cyberspace. Cyber operations causing damage, injury, or a loss of functionality of another state's governmental or private cyber infrastructure qualify as a violation of sovereignty. Furthermore, cyber operations that interfere with inherently governmental functions also amount to a violation of the target state's sovereignty. Correspondingly, cyber operations constitute illegal interventions if they intervene in another state's internal or external affairs by coercive means, such as altering electronic ballots to impact the outcome of another state's election.

The classified nature of state cyber activity makes it challenging to determine the existence of *opino juris* and state practice. Despite technical leaps and increasing public state attribution, holding states legally responsible for their malicious cyber operations remains difficult. No state

has claimed responsibility for a cyber operation or tried to publicly justify their unlawful cyber activity. States seemingly launch cyber operations with impunity, along with the knowledge or suspicion that their behavior will not trigger a response, certainly not a kinetic one. States conducting or supporting cyber operations have consistently denied the allegations or remained silent on the matter. A greater predicament is the failure of the accusing states to condemn malicious cyber operations as violations of international law, instead labelling the activity as flagrant violations of international norms or harmful conduct.

Key words: Attribution, cyberspace, cyber attack, cyber operations, non-intervention, state responsibility, internationally wrongful acts, ICTs, sovereignty, Tallinn Manual 2.0

Date: 02.11.2020	Number of pages: 88 Number of words (excl. bibliography and annexes: 34460

The abstract is approved as a maturity test:

LIST OF ABBREVIATIONS

CCD COE	NATO Cooperative Cyber Defence Center of Excellence
DDoS	Distributed Denial of Service
ICJ	International Court of Justice
ICT	Information and Communications Technology
IGE	International Group of Experts
ILC	International Law Commission
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
OPCW	Organisation for the Prohibition of Chemical Weapons
OSCE	Organization for Security and Co-operation in Europe
SCADA	Supervisory Control and Data Acquisition
UN	United Nations
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UN OEWG	United Nations Open-ended Working Group
WHO	World Health Organization

TABLE OF CONTENTS

1. Introduction

1.1 Overview

The predicament of malicious cyber operations is widely acknowledged[1]– cyberspace has become a theater of conflict where political, economic and military conflicts are being carried out.[2] Malicious cyber activities have become an everyday occurrence and there is an abundance of claims in current news headlines where cyber operations allegedly originating from inside one state's territory causes injuries within another.[3] In October 2019, the National Cyber Security Centre (NCSC) of the United Kingdom revealed in its annual review that the nation had dealt with nearly 1,800 cyber attacks in the past three years (on average ten a week), most of which were conducted by state sponsored hackers.[4] Correspondingly, Israel is reportedly on the receiving end of over 1,000 cyber attacks every minute.[5] At the time of writing, a noteworthy example of a malicious cyber operation is from April 2020, where Iranian government-backed hackers attempted to break into accounts belonging to staff at the World Health Organization (WHO).[6] Similarly, suspected Russian cyber operations have targeted organizations in Canada, the United Kingdom and the United States, involved in the development and testing of COVID-19 vaccines.[7] Furthermore, since the start of the novel coronavirus pandemic,

[1] Eric Talbot Jensen, Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017), p. 1556. Furthermore, since 2006, the Center for Strategic & International Studies (CSIS) has identified over 400 significant cyber incidents, with focus on cyber attacks on "government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars." See https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents. Also for a full list and summary of the cyber incidents, please consult the beforementioned website.

[2] Andrew Liaropoulos, 'Power and Security In Cyberspace: Implications for The Westphalian State System' (2011), p. 541.

[3] Eric Talbot Jensen, 'State Obligations in Cyber Operations' (2014), p. 1.

[4] The National Cyber Security Centre (NCSC) Annual Review 2019, p. 48, available at https://www.ncsc.gov.uk/news/annual-review-2019. See also Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention' (2019), p. 3, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

[5] BBC News, Dave Lee, 'Israel tops cyber-readiness poll but China lags behind', 8 March 2012, available at https://www.bbc.com/news/technology-16787509.

[6] CSIS, Significant Cyber Incidents, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents. See also the Telegraph, James Rothwell, 'Iran accused of attempting cyberattack on World Health Organisation, 2 April 2020, available at https://www.telegraph.co.uk/news/2020/04/02/iran-accused-attempting-cyber-attack-world-health-organisation/.

[7] National Cyber Security Centre, 'Advisory: APT29 targets COVID-19 vaccine development' 16 July 2020, https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf.

WHO has reported a fivefold increase in cyber attacks,[8] with hospitals and other medical facilities in for example the United States,[9] Thailand,[10] and Europe[11] being greatly affected.[12]

During the past three decades, cyberspace has been "woven into the fabric of daily life" and is undoubtedly penetrating all aspects of modern society.[13] Consequently, in today's digitally dependent world, governments and industry are largely reliant on so called "Supervisory Control and Data Acquisition" (SCADA) systems to control critical services and vital infrastructure, such as electric grids, nuclear power systems, gas and oil production, water supply and financial services.[14] Notwithstanding the paramount role cyberspace has in present-day society, it has also become an arena for malevolent activity, vulnerabilities and threats.[15] Militaries, terrorist groups and private individuals alike have acquired the capability to conduct cyber operations, and in practice, albeit a bit simplistic, all that is required is access to a computer and an Internet connection.[16] Whilst the threats

[8] World Health Organization, News Release, 'WHO reports fivefold increase in cyber attacks, urges vigilance', 23 April 2020, available at https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. See also The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

[9] Shira Stein, Jennifer Jacobs, 'Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak', 16 March 2020, available at https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

[10] Liviu Arsene, '5 Times More Coronavirus-themed Malware Reports during March', 20 March 2020, available at https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/.

[11] See for example Sead Fadilpasic, 'Paris hospitals targeted in major cyberattack', 24 March 2020, available at https://www.itproportal.com/news/paris-hospitals-targeted-in-major-cyberattack/; Murcia Today, 'Cyber-attack threatens Spanish hospital computer systems', 24 March 2020, available at https://murciatoday.com/cyber_attack_threatens_spanish_hospital_computer_systems_1367723-a.html.

[12] Kubo Macak, Tilman Rodenhäuser & Laurent Gisel, 'Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?', 2 April 2020, available at https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/. See also Cybersecurity and Infrastructure Security Agency (CISA), 'COVID-19 Exploited by Malicious Cyber Actors', 8 April 2020, available at https://www.us-cert.gov/ncas/alerts/aa20-099a.

[13] Russell Buchan, Nicholas Tsagourias, 'Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence' (2016), p. 377.

[14] Duncan B. Hollis, 'An e-SOS for Cyberspace' (2011), p. 379.

[15] Buchan, Tsagourias (n 13), p. 337. Furthermore, in 2013, cyberthreats overtook international terrorism as the number one global threat to America, see Jorge L. Contreras, Laura DeNardis, Melanie Teplinsky, 'Mapping Today's Cybersecurity Landscape' (2013), p. 1114.

[16] Irène Couzigou, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations' (2018), p. 37.

emanating from cyberspace vary enormously and present different levels of severity,[17] to date, no one has been injured or killed as a result of a cyber operation.[18]

Moreover, the malicious cyber activities, conducted by both state and non-state actors, are causing significant losses worldwide.[19] For instance, the WannaCry operation crippled an estimated 200,000 computers in at least 150 countries, resulting in an economic loss of approximately $4 billion worldwide.[20] Despite the increasing number of economic, humanitarian and national security implications, the low visibility international law has had in regulating state cyber operations has generated great concern.[21] Correspondingly, António Guterres, the UN Secretary-General, has stated that the world's next major conflict will begin in cyberspace: "I am convinced that if one day [we] would have a major confrontation, it would start with a massive, massive cyber attack, not only on military installations, but some civilian infrastructure. And we do not have clarity on legal frameworks on this."[22] Whereas many states have confirmed the applicability of international law to their behavior in cyberspace,[23] thus far, however,

[17] Nicholas Tsagourias, 'The Law Applicable to Countermeasures Against Low-Intensity Cyber Operations' (2014), p. 1.

[18] Anders Henriksen, 'Lawful State Responses to Low-Level Cyber-Attacks' (2015), p. 327. However, at the time of writing, the German police have launched a homicide investigation against unknown persons after a patient died as a result of a cyber attack against a hospital in Düsseldorf. The cyber attack disabled the hospital's computer system and disconnected it from the ambulance network. A critically ill patient was diverted to another hospital further away and the delay in medical treatment eventually caused the patient's life. Should the ongoing investigation lead to a prosecution, it would constitute the first ever confirmed case in which a person has died as a direct consequence of a cyber operation. Joe Tidy, 'Police launch homicide inquiry after German hospital hack', 18 September 2020, https://www.bbc.com/news/technology-54204356; The Guardian, 'Prosecutors open homicide case after cyber-attack on German hospital', 18 September 2020, https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital; The Local, 'German experts see Russian link in deadly hospital cyber attack', 22 September 2020, https://www.thelocal.de/20200922/german-experts-see-russian-link-in-deadly-hospital-hacking.

[19] Duncan B. Hollis, 'International Law and State Cyber Operations: Improving transparency' (2018), p. 1, http://www.oas.org/en/sla/iajc/docs/CJI_doc_570-18.pdf.

[20] Kapersky, 'What is WannaCry ransomware?', https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. The global ransomware attack WannaCry will be analysed in greater detail in chapter 3 of the present thesis.

[21] Duncan B. Hollis, 'Improving Transparency: International Law and State Cyber Operations: Fourth Report' (2020), p. 1, http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1.pdf.

[22] Nicholas Thompson, 'UN Secretary-General: US-China Tech Divide Could Cause More Havoc Than the Cold War', 15 January 2020, https://www.wired.com/story/un-secretary-general-antonio-guterres-internet-risks/.

[23] See e.g. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, para. 19 (June 24, 2013); Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security, UN Doc. A/70/174, para. 24 (July 22, 2017).

efforts to delineate *how* states understand international law's application to cyber operations have had limited success.[24]

Up until recently, the discussion on how international law applies to cyberspace has to a significant extent revolved around how the rules on the use of force or the law of armed conflict can govern malicious state cyber activities that result in physical damage or injuries.[25] This has resulted in an unwarranted militarization of the threats and challenges emanating from cyberspace.[26] Notwithstanding the real threat posed by cyber armed attacks and cyber warfare,[27] they are, however, not the type of hostile cyber threats that states must deal with on a daily basis.[28] The majority of the publicly known malicious cyber activities occur during peacetime,[29] and therefore have no apparent connection to an armed conflict, and seldom constitute new armed conflicts as such.[30] In 2015, only 2.4 % of all cyber operations were conducted in the context of an armed conflict or gave rise to a sufficient level of physical damage qualifying as a use of force.[31] As of March 2020, the corresponding percentage had dropped to 1.32 %.[32] Accordingly, cyber warfare is

[24] Hollis (n 19), p. 1.
[25] Harriet Moynihan, 'Power Politics Could Impede Progress on Responsible Regulation of Cyberspace', 3 December 2019, https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace?gclid=EAIaIQobChMIrYfMtq7C6QIVhqsYCh3aXAecEAAYASAAEgLqYfD_BwE
[26] Henriksen (n 18), p. 327.
[27] Cyber warfare has been vigorously debated in international fora, but the world is yet to witness a fullscale cyberwar conducted entirely in or throughout cyberspace. To date, no state has claimed that a cyber operation conducted against them has risen to the level of an armed attack and thus giving the state legal justification to exercise its inherent right to self-defense under article 51 of the UN Charter. While the law of armed conflict certainly provides effective guidelines for governing the most severe cyber operations, it would ultimately only apply to a minority of cases. The scope of the thesis is therefore strictly limited to examining peacetime cyber operations. For further information, see e.g. Michael N. Schmitt (ed.), 'Tallinn Manual on the Law Applicable to Cyber Warfare' (2013).
[28] Michael N. Schmitt (ed.), 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2017), p. 1.
[29] Katharina Ziolkowski (ed.), 'Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy' (2013), p. XV.
[30] The International Committee of the Red Cross (ICRC), 'The Potential Human Cost of Cyber Operations' (2018), p. 10. Available at https://reliefweb.int/sites/reliefweb.int/files/resources/the-potential-human-cost-of-cyber-operations.pdf. See also François Delerue, 'State Responses to Cyber Operations' (2017), p. 2.
[31] Beatrice Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law' (2017), p. 1463. See also Paolo Passeri, '2015 Cyber Attacks Statistics', HACKMAGEDDON, 11 January 2016, https://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/.
[32] Paolo Passeri, 'Q1 2020 Cyber Attacks Statistics' HACKMAGEDDON, 14 April 2020, https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/.

"only the tip of the iceberg, as an entire world of cyber operations below the threshold of cyberwarfare lies submerged."[33]

Possible threat scenarios emanating from cyberspace have ranged from computer viruses incapacitating international stock markets, to malicious code causing nuclear reactor shutdowns, to airplanes plummeting down from the sky due to a blackout in the air traffic control systems.[34] Fortunately, these dire, almost apocalyptic scenarios of an impending "cyber Pearl Harbor" do not reflect the situation as it is today.[35] Subsequently, more commonplace are persistent cyber operations, that may not be physically destructive but are nonetheless capable of damaging a state's capacity to control its critical infrastructure, often with serious economic ramifications. [36] These cyber activities are referred to as "below the threshold" cyber operations, as coined by Michael Schmitt.[37] Such cyber activity might include for instance destroying data, sabotaging cyber infrastructure, or disrupting the network of another government's websites, as was the case in Finland in 2019, when a cyber operation rendered several Finnish public service websites inaccessible, including those of the Finnish Police, the Finnish Border Guard, the Social Insurance Institution, as well as the Tax Administration and Population Centre.[38]

---

[33] François Delerue, 'State Responses to Cyber Operations' (2017), p. 4.
[34] Oona A. Hathaway, Rebecca Crootof, 'The Law of Cyber-Attack' (2012), p. 823.
[35] Zhixiong Huang, Kubo Macak, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches' (2017), p. 2. See also, Sean Lawson, 'Does 2016 Mark the End of Cyber Pearl Harbor Hysteria?', 7 December 2016, https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#39dc0bed22c2: "For twenty five years of the seventy five since Pearl Harbour, we have been talking about a digital Pearl Harbour. It still hasn't happened, so we are probably missing the point."
[36] Harriet Moynihan, 'Power Politics Could Impede Progress on Responsible Regulation of Cyberspace', 3 December 2019, https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace?gclid=EAIaIQobChMIrYfMtq7C6QIVhqsYCh3aXAecEAAYASAAEgLqYfD_BwE
[37] Michael N. Schmitt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014). Cyber operations that do not amount to the use of force have also been referred to as 'low-level' or 'low-intensity' cyber operations.
[38] YLE News, 'DoS attack downs public service websites', 22 August 2019, https://yle.fi/uutiset/osasto/news/dos_attack_downs_public_service_websites/10933436. It was widely speculated, albeit never confirmed, that Russia was behind the attacks, since they coincided with the Russian President, Vladimir Putin's visit to the Finnish capital. See also Gerard O'Dwyer, 'Finland's security agencies collaborate after cyber attacks', 29 August 2019, https://www.computerweekly.com/news/252469691/Finlands-security-agencies-collaborate-after-cyber-attacks.

1.2 Structure and delimitations

Cyber operations among states are intensifying with regard to damage and impact,[39] demonstrating that injury to critical infrastructure has become the new normal.[40] The intricate nature of cyberspace offers states a novel medium through which they can navigate and conduct malicious cyber activities, without being hindered by geopolitical borders and territorial boundaries.[41] Therefore, cyberspace does not only defy traditional principles of international law, it also offers states a "fertile terrain for gray-zone confrontation."[42] Accordingly, some states use cyber capabilities to strike with impunity, knowing or strongly convinced that their malevolent cyber activity will not trigger a response, especially not a kinetic one.[43] For instance, in the 2015 Report from the UN-mandated group of governmental experts (UN GGE), it was agreed upon that states "should not conduct or knowingly support ICT activity contrary to its 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."[44] Yet, in the case of the WannaCry ransomware attack, the operation clearly impaired the use of critical infrastructure when it severely disrupted the functioning of hospitals in the United Kingdom.[45] Despite being publicly attributed to North Korea,[46] no measures of accountability were taken against Pyongyang,[47] and no affected state explicitly claimed that the cyber operation would have been in violation of international law.

---

[39] Dennis Broeders, Bibi van den Berg (ed), 'Governing Cyberspace: Behavior, Power, and Diplomacy (2020), p. 1.
[40] Piret Pernik, 'Responding to "the Most Destructive and Costly Cyberattack in History", International Centre for Defence and Security, February 28, 2018, https://icds.ee/responding-to-the-most-destructive-and-costly-cyberattack-in-history/
[41] Gary Corn, 'Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace' (2017), p. 2.
[42] Ibid.
[43] William C. Banks, 'Symposium on Cyber Attribution: The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019), p. 191.
[44] UN GGE 2015 report, A/70/174, para. 13 (f).
[45] BBC News, 'NHS cyber-attack: GPs and hospitals hit by ransomware', 13 May 2017, https://www.bbc.com/news/health-39899646.
[46] See e.g. Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, December 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacrymalware-attack-to-north-korea-121917/.
[47] Michael J. Adams, Megan Reiss, 'How Should International Law Treat Cyberattacks like WannaCry?', 22 December 2017, Lawfare, https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry.

"Below the threshold" cyber operations such as WannaCry bring the question of state obligations in cyberspace to the foreground. Was the North Korean cyber activity in conformity with its obligations under international law? Despite the increasingly common and coercive nature of state cyber operations, locating the precise source of illegality is not always straightforward. More importantly, the exact legality of cyber operations is up to debate and they are not *per se* prohibited by international law.[48] Despite the absence of a general prohibition on cyber operations, however, in this thesis, the author's main hypothesis is that cyber operations falling below the threshold of an armed conflict or prohibited use of force can constitute a violation of a state's sovereignty or the principle of non-intervention, and thus amounting to an internationally wrongful act under the customary international law of state responsibility. Moreover, one of the most central legal issues with respect to cyberspace is *when* a cyber operation directed at a state violates its sovereignty. In essence, the thesis aims to answer the following questions:

1) When and under what circumstances do cyber operations conducted against another state violate the sovereignty of the latter?
2) How do cyber operations violate the principle of non-intervention into the internal or external affairs of another state?
3) How can cyber operations be attributed to responsible state?
4) What lawful remedies are available for injured states falling victim to a malicious cyber operation?

The regime of international responsibility comes into play when a legal subject does not conform with its legal obligations. In the cyber context, the question of how to invoke state responsibility to cyber operations has been recognized as a considerable hurdle,[49] as well as an underdeveloped part of international cyber law, especially in cases where states are believed to be the responsible entity behind a malicious cyber operation.[50] Confirming that an organ of a state originated a cyber operation can be extremely challenging even when launched from governmental infrastructure. Conversely, the mere fact that a cyber

[48] François Delerue, 'Cyber Operations and International Law' (2020), p. 193.
[49] See e.g. Scott J. Shackelford, 'State Responsibility For Cyber Attacks: Competing Standards For A Growing Problem' (2010).
[50] William Banks, 'State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0* (2017), p. 1943.

operation has been launched from (or otherwise originates from) governmental infrastructure is not sufficient evidence for attributing the operation to a state.[51]

Indeed, while many of the technical details of cyber operations are irrelevant when analyzing the application of international law, it is, however, paramount to define some general technical aspects regarding cyber operations and cyberspace. Accordingly, as this thesis aims to analyze the applicable international law in the cyber domain, the technical jargon might prove extremely rudimentary to those familiar with information and communications technology (ICT). Moreover, a brief overview and analysis of the most infamous cyber operations to date will follow. The WannaCry operation, already briefly mentioned in the introduction, is considered the "the largest ransomware attack observed in history"[52] and will be used as a significant case study. However, in order to illustrate the broad spectrum of malicious cyber activity, more small-scale cyber operations will be presented throughout the thesis.

The following topics will be discussed in turn: Chapter 2 seeks to give the reader some analytical clarity and aims to shine some light on the different state cyber activities taking place in cyberspace. Cyberspace can be viewed as a fusion of "all communication networks, databases and information sources into a global virtual system,"[53] and is composed of three separate and intertwined layers. Furthermore, the chapter sets out the *status quo*, providing a discussion on the legal status of cyberspace and how international law applies therein. Subsequently, since cyberspace requires a physical infrastructure to function, it is not disjoined from state sovereignty. The thesis then turns to analyzing the legal requirements of holding a state responsible for a malicious cyber operation. Accordingly, chapter 3 will seek to apply the existing rules of state responsibility to cyber operations and elaborate on how cyber operations can constitute internationally wrongful acts. The chapter will also provide a brief introduction of the notion of state sovereignty and its application to state cyber activities. As will become apparent, disputes regarding the application of sovereignty in cyberspace have emerged, and the diverging state views will be analyzed. For instance, it is the view of the United Kingdom, that a cyber operation

[51] Michael Schmitt (ed.), ''Tallinn Manual on the International Law Applicable to Cyber Warfare' (2013), rule 7 – Cyber Operations Launched from Governmental Cyber Infrastructure, p. 39.
[52] BBC, 'NHS cyber-attack: No 'second spike' but disruption continues', 15 May 2017, https://www.bbc.com/news/uk-39918426.
[53] Liaropoulos (n 2), p. 541.

conducted into another state's territory cannot amount to an internationally wrongful act on the basis of having violated that state's sovereignty. Chapter 4 will delve to analyze the attribution mechanism of cyber operations and whereas chapter 5 will provide an evaluation on possible state responses available for injured states. Finally, the final chapter will provide concluding thoughts and reiterate the most important parts from the thesis, as well as answering the question whether extant international law is adequate to regulate state behavior in cyberspace, or whether a separate cyber specific regime would be more adequate for holding states accountable for their malicious cyber activities.

An immediate challenge for any discussion of cyber related issues, whether at a political, technical or legal level, is the lack of a commonly accepted vocabulary.[54] This has been echoed by Professor Michael Schmitt, who has stated that "the greatest hindrance to effective conversation between cyber norm communities is terminological in nature."[55] It should also be kept in mind that the "mixing of legal terminology with colloquial discourse can have important ramifications for the application of the law, and as a result, for the protection of persons, preservation of state authority, and stability of the international system."[56] "Cyber attack" is perhaps the most commonly used term to describe malicious activity in cyberspace.[57] However, it is paramount to underline that the usage of cyber attack throughout this thesis must not be interpreted in the military sense of the word.

As a starting point, the definition of cyber operation provided by the International Group of Experts (IGE) in the "Tallinn Manual 2.0 on The Law Applicable to Cyber Operations" (hereinafter referred to as Tallinn Manual 2.0[58]) will be used, and the definition is as follows: "[t]he employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."[59] The objectives may include physical

[54] Corn (n 41), p. 1.
[55] Michael Schmitt, Liis Vihul, 'The Nature of International Cyber Norms' (2014), p. 6.
[56] Laurie R. Blank, 'Cyberwar/Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' (2014), p. 2.
[57] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012), p. 229.
[58] See Chapter 1.3.
[59] Tallinn Manual 2.0, p. 564.

damage,[60] as well as economic or political disruption.[61] However, due to the sake of non-repetition, these terms, that connotate a relationship with information technology,[62] will be used interchangeably throughout, as a catchall for any malicious "computer-network attack or computer-based actions"[63] conducted in peacetime. More importantly, the terms will be used to denote *state* cyber operations, that is cyber operations conducted by a state or otherwise attributable to that state under the International Law Commissions' Draft Articles on State Responsibility.[64] Cyber operations conducted by non-state actors will be touched upon only for the purpose of determining when and if they can be attributed to a state.

1.3 Materials and methods

The complex nature of cyberspace has sparked considerable uncertainty about the application of existing international legal frameworks.[65] A great deal of the present day domestic and international legal system is built upon certain basic principles, for instance the sovereign equality of states and related concepts of sovereignty such as the principle of non-intervention, as well as the notion of state responsibility – cyberspace inherently challenges each of these premises.[66]

In 1996, John Barlow stated in his notorious "Declaration of the Independence of Cyberspace" that legal concepts do not apply in the cyber domain.[67] Howbeit, at this day and age, it is no longer seriously argued that state activities in cyberspace fall entirely

[60] Jiang Zhifeng, 'Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal' (2019), p. 60.
[61] See e.g. Barrie Sander, 'Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019), where the alleged Russian meddling in the 2016 US Presidential election was described as "the political equivalent of 9/11".
[62] Tallinn Manual 2.0, p. 564.
[63] Thomas Payne, 'Teaching Old Law New Tricks: Applying and Adapting State Responsibility To Cyber Operations' (2016), p. 691.
[64] The responsibility of international organizations will fall outside the scope of this thesis. For a discussion of the latter, see e.g. Tallinn Manual 2.0, pp. 153-167.
[65] Corn (n 41), p. 8. See also Michael Schmitt, Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum' (2018), p. 242.
[66] Corn (n 41), p. 8.
[67] John Barlow, 'A Declaration of Independence for Cyberspace' (1996), available at https://scholarship.law.duke.edu/dltr/vol18/iss1/2/.

outside the scope of the traditional international law framework.[68] The applicability of international law to cyberspace has been widely discussed in international fora. For example, it has been maintained in two consecutive reports of a UN-mandated group of governmental experts (UN GGE[69]) that international law (including the UN Charter) is applicable to cyberspace.[70] Furthermore, the European Union,[71] North Atlantic Treaty Organization (NATO),[72] the Organization for Security and Co-operation in Europe (OSCE)[73] as well as individual states[74] have confirmed that international law applies in cyberspace.

Extant rules of international law will be systemized, interpreted, and applied to the context of cyberspace, using a legal dogmatic approach. In other words, the pressing issue at hand is the precise manner in which "pre-cyber" international law is to be applied in the cyber context. A starting point for any consideration of the legal architecture of the international community, as well as the applicable law to state activities in cyberspace, is irrefutably Article 38 (1) of the Statute of the International Court of Justice (ICJ Statute).[75] In the

[68] Kubo Macak, 'On The Shelf, But Close At Hand: The Contribution of Non-state Initiatives to International Cyber Law' (2019), p. 81.
[69] Since 2004, six Groups of Governmental Experts (GGE) have examined the threats posed by the use of Information and Communication Technologies (ICTs) in the context of international security; 2004/2005 (A/RES/58/32), 2009/2010 (A/RES/60/45); 2012/2013 (A/RES/66/24); 2014/2015 (A/RES/68/243); 2016/2017 (A/RES/70/237); 2019/2021 (A/RES/73/266). See https://www.un.org/disarmament/ict-security/ and https://dig.watch/processes/un-gge.
[70] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, para. 19 (June 24, 2013); Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security, UN Doc. A/70/174, para. 24 (July 22, 2015).
[71] Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 20 November 2017, para. 5, https://www.consilium.europa.eu/media/31666/st14435en17.pdf,
[72] North Atlantic Treaty Organization (NATO), Wales Summit Declaration (Issued by the Head of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014, para.72, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.
[73] Organization for Security and Co-operation in Europe (OSCE), Permanent Council Decision No. 1202, OSCE Confidence-Building Measures To Reduce The Risks of Conflict Stemming From The Use of Information And Communication Technologies, 10 March 2016, PC.DEC/1202, https://www.osce.org/pc/227281.
[74] See e.g. the Netherlands: Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, available at 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; France: Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberspace', 9 September 2019, available at https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.
[75] Statute of The International Court of Justice, art.38 (1), 26 June 1945, 59 Stat. 1055, 33 UNTS 993; Schmitt, Vihul (n 55), p. 3.

present thesis, primary legal sources will be examined together with secondary sources, as the latter will be regarded as "books and articles, purporting to answer legal questions … when ascertaining the content of international law."[76]

At the time of writing, however, there are few multilateral treaties which directly deal with cyber operations, and those that have been adopted primarily regulate cybercrime and are of a rather limited scope.[77] As no specific cyber treaty or convention exists, customary international law is of particular importance as "it occupies a position of preeminence in developing areas of the law."[78] In other words, the applicability of international law in cyberspace is largely dependent on customary international law.[79] The thesis will therefore analyze "below the threshold" cyber operations as a topic of customary international law, where the works of the International Law Commission (ICL), especially its Draft Articles on Responsibility of States for Internationally Wrongful Acts[80] (hereinafter Draft Articles) will be studied. The legal parameters of attributing a malicious cyber operation to a state and holding that state legally responsible are customary in nature and despite being unwritten rules, customary international law is widely acknowledged to be binding upon all states.

Customary international law consists of two elements – state practice and *opinio juris* – and is viewed as "evidence of general practice accepted as law."[81] A general practice refers to the fact that it is primarily the practice of states that contribute to the formation of customary international law.[82] In rudimentary terms, state practice is what nations do.

---

[76] Sondre Torp Helmersen, 'Finding 'the Most Highly Qualified Publicists': Lessons from the International Court of Justice' (2019), p. 509.
[77] Tallinn Manual 2.0, p. 3. A noteworthy treaty is the Council of Europe's Convention on Cybercrime (2001) (also known as the Budapest Convention). The convention in question was the first international agreement "aimed at reducing computer-related crime by harmonizing laws, improving investigative techniques, and increasing international cooperation." See list on Treaties and International Agreements on Cyber Crime, available at https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478. However, the number of parties to the convention (64 countries as of February 2020) and the regulatory items are of a limited scope. See Keiko Kono, 'International Laws on Cyber attacks that Do Not Constitute an Armed Attack' (2017), p. 1, available at http://www.nids.mod.go.jp/english/publication/briefing/pdf/2017/briefing_e201710.pdf.
[78] Gary Brown, Keira Pollet, 'The Customary International Law of Cyberspace' (2012), p. 126.
[79] Duncan B. Hollis, 'Elaborating International Law for Cyberspace', 29 July 2020, https://directionsblog.eu/elaborating-international-law-for-cyberspace/.
[80] The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission, 53rd session, (Apr. 23-June 1,July 2-Aug. 10, 2001), General Assembly Official Records, 56th session, supp. no. 10, UN Doc. A/56/10.
[81] ICJ Statute, art. 38 (1) (b).
[82] Kriangsak Kittichaisaree, 'Public International Law of Cyberspace' (2017), p. 18.

Including both physical and verbal acts, it consists of the conduct of the state, whether it is exercising its executive, legislative, judicial, or other functions.[83] There is also no hierarchy among the different forms of state practices. State practice can manifest itself through, *inter alia*, state acts, diplomatic exchanges, voting for or adopting resolutions in an international organization, or statements at international conferences. State practice is not only composed of actual acts, seen as inaction (acquiescence) is also evidence of state conduct.[84] The abstention from acting is also referred to as a "negative practice of States."[85]

Opinio juris is the acceptance of the conduct as law, differentiating legal duty from mere habit, courtesy or tradition.[86] In other words, for a custom to be considered as legally binding, state practice must be general and consistent and followed by a state's sense of legal obligation.[87] Evidence of *opinio juris* is primarily found in "statements of belief", such as treaty provisions or declarations, denoting the conviction of a state that the practice is legally obligatory.[88]

An increasing amount of state cyber practice has emerged, and states have begun issuing their views on the applicability of international law in cyberspace. However, custom does not appear instantaneously, but rather through consistent state practice. Therefore, the thesis scrutinizes available state cyber practice and *opinio juris* in order to determine to what extent customary international law has developed and governs state behavior in cyberspace.

It is therefore paramount to acknowledge and contextualize the individual national views on international law in cyberspace. During the past few years, several states have publicly issued national statements on the application of international law to cyberspace, most

[83] Ibid.
[84] See e.g. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports (1996), para. 65: "States which hold the view that the use of nuclear weapons is illegal have endeavoured to demonstrate the existence of a customary rule prohibiting this use. They refer to a consistent practice of non-utilization of nuclear weapons by States since 1945 and they would see in that practice the expression of an *opinio juris* on the part of those who possess such weapons."
[85] International Law Commission, 'Second report on the identification of customary international law', 22 May 2014, UN/A/CN.4/672, https://legal.un.org/ilc/documentation/english/a_cn4_672.pdf
[86] Kittichaisaree (n 82), p. 19.
[87] Brown, Pollet (n 78), p. 126.
[88] Ibid, p. 128; Kittichaisaree (n 82), p. 19.

recently Finland in October 2020.[89] While the statements issued are predominantly from European countries (with the exceptions of The United States and Australia), Iran has also recently published its views on how international law applies in cyberspace.[90] Apart from China and Russia, Iran is the first major non-Western cyber power to have released such a statement.[91] Conversely, the published national positions on the applicability of international law to malicious cyber operations differ to a considerable extent, not only between, for instance, the United States and Russia, but also among Western, like-minded states and even between NATO allies.[92]

Similarly, by the beginning of 2019, nearly 90 states had adopted a national cyber security strategy.[93] As they may contain possible strong evidence of the norms two which states deem themselves to be legally bound by, the present thesis will examine the national strategies of *inter alia* France, the Netherlands, the United States, the United Kingdom, Russia, and China. However, the analysis is not strictly limited to the aforementioned states, as other examples will be referred to in relevant passages.

A considerable amount of state cyber operations is of a highly classified nature, or in some ways hidden from the watchful eyes of other states. This predicament is troubling, since state practice that is not visible does not contribute to the formation of new customary international law.[94] How are states to be held accountable for malicious cyber activity that is not visible?

---

[89] Finnish Ministry for Foreign Affairs, 'Finland published its positions on public international law in cyberspace', 15 October 2020, https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace. Official English translation: International law and cyberspace – Finland's national positions, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

[90] General Staff of the Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat, 18 August 2020, available on https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

[91] Przemyslaw Roguski, 'Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace', Just Security, 3 September 2020, https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/.

[92] Eneken Tikk, 'International Law in Cyberspace: Mind the gap' (2020), Cyber Policy Institute, https://www.helsinki.fi/sites/default/files/atoms/files/tikk_2020_international_law_in_cyberspace.pdf, p. 10.

[93] Ann Väljataga, 'Tracing *opinio juris* in National Cyber Security Strategy Documents' (2018), NATO CCDCOE, p. 18.

[94] Michael N. Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace' (2020), p. 36.

As non-binding instruments may be influential and contribute to the development of customary international law, UN GGE Reports and UN Open-ended Working Group (OEWG) Reports will be referred to throughout. Another important source used in this thesis is the Tallinn Manual 2.0.[95] Keeping in mind that the Tallinn Manual 2.0 cannot be equated to the primary sources of international law, it will however, in this thesis, be regarded as "teachings of the most qualified publicists".[96] It is to date the most detailed contribution in the cyber law area – in its nearly 600 pages and 154 rules (followed by extensive commentary), the Tallinn Manual 2.0 lays out the general legal principles that govern cyber operations and their interaction with specialized international legal regimes, e.g. international human rights law.[97] All the rules were adopted using a consensus approach within the International Group of Experts (IGE).[98] More importantly, the experts agreed that upon successfully adopting a rule it would reflect customary international law, provided that the rule was not already covered in a treaty.[99]

A focal point of criticism levelled at the Tallinn Manual 2.0 is the claim by some states (especially Russia and China) that it primarily represent the official views of Western states.[100] Conversely, despite having been labeled "NATO doctrine",[101] it must be kept in mind that it is neither an intergovernmental agreement nor official document, but rather an academic product of independent experts acting solely in their personal capacity, and should be regarded as an attempt by distinguished international lawyers to facilitate the

[95] Michael Schmitt (ed.), 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2017).
[96] ICJ Statute, art. 38(1)(d).
[97] In total, the Tallinn Manual 2.0 is divided into four major parts: general international law and cyberspace; specialized regimes of international law and cyberspace; international peace and security and cyberspace; and the law of cyber armed conflict.
[98] Tallinn Manual 2.0, p. 4.
[99] Tallinn Manual 2.0, p. 4. It was further noted that "to the extent the rules accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors." (ibid).
[100] Kono (n 77), p. 1. Both editions of the Tallinn Manuals have generated considerable reaction in the international community, ranging from praise to condemnation. See e.g. Gary Corn, 'Tallinn Manual 2.0 – Advancing the Conversation', 15 February 2017, Just Security, calling the work of the IGE "significant and admirable", available at https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/; Michael J. Adams, 'A Warning About Tallinn 2.0 … Whatever It Says', 4 January 2017, LAWFARE, available at https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says.
[101] Michael Schmitt, 'Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't', 9 February 2017, Just Security, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/.

regulation of cyber operations by international law.[102] Nonetheless, given the above, it can be concluded that the Tallinn Manual 2.0 will:

> serve as a primary reference source for analyzing States' international legal rights and responsibilities when operating in cyberspace outside of armed conflict to achieve national objectives and confront the growing threats posed by both state and non-state actor cyber operations below the use-of-force threshold.[103]

[102] Dan Efrony, Yuval Shany, 'A Rulebook on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice (2018), p. 583. However, during the drafting process of Tallinn Manual 2.0, over fifty states provided unofficial feedback. See CCDCOE, 'Over 50 States Consult Tallinn Manual 2.0'. 2 February 2016, https://ccdcoe.org/news/2016/over-50-states-consult-tallinn-manual-2-0/. Furthermore, during the CCDCOE's 4th International Conference on Cyber Conflict, Michael Schmitt stated that the Tallinn Manual 1.0 is "a restatement of the law, it does not make law." 'CyCon 2012, Michael Schmitt: Tallinn Manual part 1', available https://www.youtube.com/watch?v=wY3uEo-Itso.

[103] Gary Corn, 'Tallinn Manual 2.0 – Advancing the Conversation', 15 February 2017, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

2. Technical and legal aspects of cyberspace

2.1 Concepts and terminology

When describing malicious cyber activity, generic terms such as, cybercrime, cyber attack, cybersecurity, are regularly used interchangeably without any distinction.[104] As this inevitably creates confusion and misunderstandings, it is paramount to discuss and establish a baseline understanding of the most central terms covered in this thesis. First and foremost, the initial matter is defining what is meant by the term "cyberspace", since it has "political, economic and cultural aspects going far beyond the notion of a pure means of information transfer."[105]

The notion of cyberspace – coined around three decades ago by William Gibson[106] – can be viewed as "to cover all entities that are or may potentially be connected digitally."[107] Howbeit disagreements about the nature and regulation of cyberspace are nothing new,[108] and even though cyberspace "has become a mainstay of twenty-first century commerce and society, the terminology to describe it is still developing."[109] Hence the objective of the chapter is twofold. Firstly, the chapter endeavors to provide a basic technical understanding of cyberspace and its features, and secondly, it will focus on the legal representation of cyberspace and its current status in international law. Furthermore, after having provided a basic technical and legal understanding of cyberspace, the remainder

[104] Terminology also posed particular obstacles during the drafting process of Tallinn Manual 2.0. Thus, many commonly used words have a specific military legal meaning. For example, the word 'attack' "refers in common usage to a cyber operation against a particular object or entity, and in the military sense it usually indicates a military operation targeting a particular person or object. However, attack in the *jus ad bellum* sense, qualified by the word 'armed', refers to a cyber operation that justifies a response in self-defence." See Tallinn Manual 2.0, pp. 4-5.
[105] Katharina Ziolkowski (ed.), 'Peacetime Regime for State Activities in Cyberspace' NATO CCD COE Publication, (2013), p. 170.
[106] The word "cyberspace" is credited to William Gibson and his book Neuromancer (1984), where he describes cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation. A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data." See https://techterms.com/definition/cyberspace; Paul Ducheine, Peter Pijpers, 'The Notion of Cyber Operations' (2020), p. 2.
[107] Netherlands Defence Cyber Strategy (2012), quoted in Paul Ducheine, Peter Pijpers, 'The Notion of Cyber Operations' (2020), p. 2.
[108] Scott J. Shackelford, 'Governing New Frontiers in the Information Age: Toward Cyber Peace' (2020), p. 21.
[109] Ibid.

of the chapter seeks to give the readers clarity vis-à-vis "below the threshold" cyber operations.

2.2 The notion of cyberspace

Hic sunt leones – "here be lions," was an expression used by Roman and medieval cartographers to describe uncharted territories and the possible dangers within.[110] The expression would be a suitable way of describing cyberspace if it were a real physical location appearing on geographical maps.[111] Conversely, cyberspace does not belong to any one state, much like the high seas or international airspace, and it stands to reason that the traditional Westphalian nation state boundaries were not drawn with cyberspace in mind. However, despite being a fluid and fastmoving realm without a central authority, cyberspace does not constitute a lawless Wild West, a characterization that the international community has worked vigorously on to put to rest.[112]

The Internet – "the global public memory" – is often referred to as cyberspace, and it has rapidly become the backbone of almost everything in society – not only as regards to human communication, social media or entertainment, but also healthcare, air traffic, sewage, electrical grids, education and mass transit have become crucially reliant on the Internet to facilitate their everyday process. Furthermore, the Internet has a profound impact on the way states deliver their core functions of *inter alia* ensuring peace and security, economic and social wellbeing as well as the protection of fundamental human rights.[113] As of April 2020, there were an estimated 4.57 billion Internet users worldwide, amounting to 59 % of the total global population.[114] With this considerable amount of people relying on the Internet for a variety of economic, social, and political

[110] Marco Roscini, 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force' (2010), p. 86.
[111] Ibid.
[112] Schmitt (n 94), p. 33.
[113] Jovan Kurbalija, 'State Responsibility in Digital Space' (2016), p. 308.
[114] Statista, Worldwide digital population as of April 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/. Last accessed 29 April 2020. Moreover, there is an estimated 26 billion devices connected to the Internet. See Jacob Morgan, 'A Simple Explanation of 'The Internet Of Things', 13 May 2014, Forbes, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7ca2a4f01d09. See also Kersti Kaljulaid, President of the Republic Opening Speech at CyCon 2017, 31 May 2017, https://www.president.ee/en/official-duties/speeches/13324-president-of-the-republic-opening-speech-at-cycon-2017-31-may-2017/index.html, stating that the number of devices connected to the Internet has already far exceeded the number of devices one would traditionally call computers.

interactions,[115] cyberspace is "nothing short of essential to modern life."[116] Cyberspace has also been perceived as a "common heritage of mankind", and access to its benefits constituting a legitimate right for all peoples.[117]

However, in light of the above, and contrary to popular belief, the Internet is not tantamount to cyberspace[118] - it extends far beyond.[119] While the Internet does constitute the main component of cyberspace, it also includes "other networks of computers, including those that are not supposed to be accessible from the Internet."[120] Consequently, cyberspace can generally be understood as a global, intangible space, electronic medium, consisting of both physical and technical components, that are contained on publicly accessible websites, as well as all the entities and individuals connected to the Internet.[121] According to the Tallinn Manual 2.0, cyberspace is viewed as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."[122]

Cyberspace is made up of three different layers – physical, logical and social[123] – within or against which cyber operations can be conducted.[124] Moreover, at any given moment, the "the operationally relevant components of each layer reside somewhere on the globe, usually within the sovereign territory or subject to the control of at least one state."[125] Furthermore, the Tallinn Manual 2.0 specifically provides that "the physical, logical and social layers of cyberspace are encompassed in the principle of sovereignty."[126]

---

[115] In 2005, Estonia became the first country in the world to hold nationwide elections using the so called i-Voting. Similarly, in 2007, Estonia made worldwide headlines as the first country to use electronic voting in parliamentary elections. Furthermore, it is noteworthy to add that 99% of Estonian public services are online 24/7. See https://e-estonia.com/solutions/e-governance/i-voting/.
[116] Melanie Teplinsky, 'Fiddling on the Roof: Recent Developments in Cybersecurity' (2013), p. 228.
[117] Ahmad Kamal, 'The Law of Cyber-space: An Invitation to The Table of Negotiations, (2005), p. 4.
[118] Emilie Legris, Dimitri Walas, 'ESIL Reflection: Regulation of Cyberspace by International Law' (2018), https://esil-sedi.eu/fr/esil-reflection-regulation-of-cyberspace-by-international-law/.
[119] Barrie Sander, 'Cyber Insecurity and the Politics of International Law' (2017), https://esil-sedi.eu/post_name-1148/.
[120] Henriksen (n 18), p. 329. See also Andrew Liaropoulos, 'War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory' (2010), p. 181.
[121] Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' (2013), p. 135.
[122] Tallinn Manual 2.0, p. 564.
[123] Tallinn Manual 2.0, p. 12.
[124] Corn (n 41), p. 9.
[125] Ibid.
[126] Tallinn Manual 2.0, p. 12.

The *physical* layer of cyberspace is made up of the physical network components as well as the geographic component.[127] The physical network component consists of the components needed to store, transport and process information within cyberspace, such as computers, routers and servers.[128] The geographical component, on the other hand, refers to the physical location of the network. The physical network constitutes a first point of reference that can be used to determine the geographical location of the elements of the network, as well as the appropriate legal response should the network be used to conduct malicious cyber activities.[129] Cyberspace is *de facto* transnational by nature and can therefore raise several issues relating to sovereignty and jurisdiction. Whereas the core of cyberspace is made up of virtual factors, it is nonetheless supported by physical, tangible objects such as computers, which connect "the irreducible part of cyberspace to the physical world; and interactions in cyberspace are independent of time or space constraints and are conducted through logistics rather than through physical acts."[130] The *logical* layer is more abstract and refers to the data, connections and protocols that exist between the physical components in cyberspace.[131] Put differently, it contains all the applications needed to store and process the data that resides in the physical layer.[132] Finally, the *social* level consists of the actors who engage in cyber activities in cyberspace.[133]

It is not surprising to see deliberations of territories and boundaries in ongoing discussions of international law in cyberspace. Accordingly, some have characterized cyberspace as a "distinct, self-governing "space", entitling it to autonomy or non-state governance" or insisted that "cyberspace is just a technological medium that states can govern by reference to national boundaries."[134] This chapter will now turn to analyzing the legal status of cyberspace and how international law applies therein.

[127] Tallinn Manual 2.0, p. 9. See also Corn (n 41), p. 9.
[128] Joint Publication 3-12, 'Cyberspace Operations', 8 June 2018, p. 3.
[129] Joint Publication 3-12, 'Cyberspace Operations', 8 June 2018, p. 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[130] Nicholas Tsagourias, 'The legal status of cyberspace' (2015), p. 15.
[131] Tallinn Manual 2.0, p. 12.
[132] Sasha Romanosky, Zachary Goldman, 'Understanding Cyber Collateral Damage' (2017), p. 235.
[133] Tallinn Manual 2.0, p. 12.
[134] Duncan B. Hollis, 'Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?' (2014), p. 2.

2.3 The legal status of cyberspace

The prefix "cyber" comes from the Greek verb "kyberno", which means to steer or to govern.[135] However, cyberspace does not have physical or geographical borders, and it therefore challenges "the law's traditional reliance on territorial borders; it is a "space" bounded by screens and passwords rather than physical markers."[136] Accordingly, the application of the existing notions of sovereignty to cyberspace has been questioned, especially due to its distinct a-territorial and borderless nature. Some scholars have rejected the possibility of applying existing principles of sovereignty to cyberspace, instead advocating the creation of discrete laws for cyberspace.[137] However, the views expressed at the "early days of legal encounters with cyberspace" have changed, and it is by now generally held that international law applies to cyberspace.[138] This has been confirmed on both an international[139] and a regional level,[140] as well as in (joint) statements of states.[141]

The debate has hence shifted to *how* international law applies in cyberspace and with what consequences. An immediate point of concern is the fact that there are very few international treaties governing and regulating cyberspace.[142] Furthermore, the classified nature of states' cyber activities makes it challenging to determine the existence of *opinio juris* and state practice therefore overseeing the development of customary law in cyberspace. In other words, as states conduct cyber operations in secret and still relatively

---

[135] Liaropoulos (n 2), p. 541.
[136] David R. Johnson, David Post, 'The Law And Borders – The Rise of Law in Cyberspace' (1996), p. 1367.
[137] "Separated from doctrine tied to territorial jurisdiction, new rules will emerge to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world." David R. Johnson & David Post, 'Law and Borders - The Rise of Law in Cyberspace (1996), p. 1367.
[138] Nicholas Tsagourias, 'Law, Borders and Territorialisation of Cyberspace' (2018), p. 13.
[139] See UN GGE 2013 report A/68/98, para. 19: "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."; UN GGE 2015 report, A/70/174: "The Group emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by States."
[140] See e.g. 'EU Cybersecurity Strategy' (2017) "The EU strongly promotes the position that international law and in particular the UN Charter, applies in cyberspace."
[141] Joint Statement on Advancing Responsible State Behavior in Cyberspace (2019), affirmed by: Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Spain, Sweden, the United Kingdom, and the United States. Statement available at e.g. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.
[142] Tallinn Manual 2.0, p. 3.

few nations have put forth their national views on international law and cyber.[143] Available state practice in relation to cyber operations suggests that it is developing along two parallel tracks "acknowledged and unacknowledged, resulting in the emergence of two sets of "rules of the game" – international law rules and softer informal rules."[144]

At an inter-state level, considerable efforts have been made to clarify how extant international law applies to state conduct in cyberspace. Since the challenges posed by the rapid developments in information and communication technologies (ICT) was brought to the attention of the international community in the late 1990s,[145] the so-called "UN GGE process" (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security) has been the primary platform for an interstate dialogue about the international legal regulation of cyberspace.[146] More specifically, cyberspace appeared on the international agenda in 1998, when Russia submitted a resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security" with the aim of initiating a negotiation process on a treaty to regulate the usage of ICTs in international conflicts,[147] fearing the "development, production or use of particularly dangerous forms of information weapons."[148] The thought of a multilateral treaty was quickly dismissed by most Western states since "cyberspace did not substantially differ

[143] To date, the following states have issued national statements: Germany: Militärische, völkerrechtliche und rüstungskontrollpolitische Aspekte der Cyber-Sicherheit (2011), Andwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare) (2015); Russia: Concept of a Convention on International Information Security (2011); United States: International Law in Cyberspace (2012), International Law and Stability in Cyberspace (2016); Australia, Australia's position on how international law applies to state conduct in cyberspace (2017), Australia's Position on the Application of International Law to State Conduct in Cyberspace (2019); the United Kingdom, Cyber and International Law in the 21st Century (2018); the Netherlands, International law in cyberspace (2019); Estonia, Estonian official positions on international law in cyberspace (2019); France, International Law Applied to Operations in Cyberspace (2019). See Tikk (n 92), p. 16.

[144] Efrony, Shany (n 102), p. 586.

[145] 'Prospects and Challenges of Developing International Cybersecurity Norms in the UN', Introductory speech by Daniel Stauffacher, 29 May 2019, available at https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf. The resolution was adopted without a vote by the General Assembly (UN Doc. A/RES/53/70 (4 January 1999)).

[146] Anders Henriksen, 'The end of the road for the UN GGE process: The future regulation of cyberspace' (2018), p. 1.

[147] Dennis Broeders, Fabio Cristiano, 'Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road', 2 April 2020, https://www.ispionline.it/it/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417.

[148] Letter dated 98/09/23 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary General, https://digitallibrary.un.org/record/261158?ln=en#record-files-collapse-header.

from the offline world and thus standing international law would be sufficient for its regulation."[149]

The GGE process began in 2004[150] and has since then consisted of five groups.[151] Furthermore, initially the GGE consisted of 15 countries, but by 2016 the number of member states had grown to 25.[152] Conversely, only three GGEs have led to consensus reports; 2010,[153] 2013,[154] and 2015.[155] Furthermore, the UN Secretary-General has stated that the recommendations contained in the 2013 UN GGE Report "point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security."[156] Moreover, the 2015 UN GGE Report further clarified the applicability of international law to cyberspace, by proposing eleven specific, non-binding international norms and principles that apply or ought to apply to cyberspace.[157] The eleven recommendations for cyber norms largely reflect extant international law[158] and they can be divided into two categories; 1) norms having a limiting character and 2) principles stating good practices and positive duties for the purpose of international security.[159] The norms provide *inter alia* that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs", [160] being the first consensus report from the UN GGE specifically using the wording "internationally wrongful act" found in the ILC's Draft Articles.

---

[149] Dennis Broeders, Fabio Cristiano, 'Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road', 2 April 2020, https://www.ispionline.it/it/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417.
[150] UN Doc A/RES/58/32. (8 December 2003).
[151] Michael Schmitt, Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms', 30 June 2017, Just Security, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
[152] The five permanent UN Security Council members have always been involved. Michael Schmitt, Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms', 30 June 2017, Just Security, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
[153] UN Doc. A/65/201 (30 July 2010).
[154] UN Doc. A/68/98 (24 June 2013).
[155] UN Doc. A/70/174 (22 July 2015).
[156] UN GGE 2013 report A/68/98, p. 4.
[157] Tsagourias (n 138), p. 14.
[158] Broeders, van den Berg (n 39), p. 25.
[159] CCDCOE, '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/
[160] UN GGE 2015 report, A/70/174, p. 8.

The task of how to implement set cyber norms in practice was left to the following UN GGE which began their work in 2016. However, in 2017, the UN GGE collapsed as a number of states (including Russia, China and Cuba) rejected the proposed text of the final report.[161] It was the first time that two states – Cuba and the United States – had put forth their views and specific reasoning behind the failure to reach a consensus.[162] The UN GGE failed to resolve the quarrelsome issue of how international law applies in cyberspace, as "moving beyond the general dictum that 'international law applies' has proven to be [a] stumbling block."[163] An American expert criticized some countries for wanting "to walk back progress made in previous GGE reports" and opining that states "who are unwilling to affirm the applicability of these international legal rules and principles believe that their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions."[164] The Cuban delegation on the other hand accused some states of attempting to "convert cyberspace into a theater of military operations"[165] by excessively focusing the discussion on international humanitarian law, the right to self-defence and countermeasures. Cuba further stated that "[t]he 'Law of the Jungle' cannot be imposed, in which the interests of the most powerful States would always prevail to the detriment of the most vulnerable."[166] Interestingly

[161] Michael Schmitt, Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms', 30 June 2017, Just Security, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
[162] Broeders, van den Berg (n 39), p. 25.
[163] Dennis Broeders, Fabio Cristiano, 'Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road', 2 April 2020, https://www.ispionline.it/it/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417.
[164] Michele Markoff, U.S. Expert to the GGE, 'Explanation of Position at the Conclusion of the 2016-201 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security', https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/.
[165] Declaration by Miguel Rodríguez, Representative of Cuba, At the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 23 June 2017, https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf. "We consider it unacceptable formulations contained in the draft, aimed to establish equivalence between the malicious use of ICTs and the concept of 'armed attack', as provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context of the right to self-defense."
[166] Ibid.

enough, in the UN GGE 2015 Report, the aforementioned states agreed to the very same principles that they rejected in the 2017 Report.[167]

After the collapse of the 2016-2017 UN GGE, some commentators went as far as declaring the whole UN process dead.[168] The UN came under increasing pressure, as the groups had been criticized for their exclusionary approach.[169] Since the groups have consisted of fifteen to twenty-five member, the considerable majority of UN member states find themselves excluded from the in-depth discussion on a matter that has rapidly become a major security concern for states around the world.[170] Moreover, the inaccessibility for a variety of non-state actors, including civil society and academia, was another focal point of criticism aimed that the GGEs. Concurrently, there have been a number of efforts in the non-governmental sector to clarify how international law applies to state behavior in cyberspace, e.g. Microsoft's call for a "Digital Geneva Convention" in 2017,[171] as well as the Global Commission on the Stability of Cyberspace (GCSC) final report in 2019.[172] Moreover, the French "Paris Call for Trust and Security in Cyberspace," has, at the time of writing, received the support of 78 states, 29 public authorities and local governments, 349 organizations and members of civil society, and 644 companies and private sector entities.[173] Thus, due to the state-centric approach of the previous GGEs, the General Assembly established two processes to further discuss the security issues in cyberspace, and the risk that the misuse of ICTs poses for the international community.[174] Hence, during the period of 2019-2021, an Open-ended Working Group

[167] Michael N. Schmitt, Liis Vihul, 'International Law Politicized: The UN GGE'S Failure to Advance Cyber Norms', Just Security, 30 June 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
[168] Alex Grisby, 'The Year in Review: The Death of the UN GGE Process?' 21 December 2017, https://www.cfr.org/blog/year-review-death-un-gge-process.
[169] François Delerue, Elaine Korzak, 'From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity', 27 January 2020, Council on Foreign Relations, https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity.
[170] Ibid.
[171] Microsoft, 'A Digital Geneva Convention to protect cyberspace', https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.
[172] Global Commission on the Stability of Cyberspace, 'Advancing Cyberstability', November 2019, available at https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.
[173] France, Ministry for Europe and Foreign Affairs, 'Paris Call for Trust and Security in Cyberspace', 12 November 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.
[174]United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/ict-security/

(OEWG)[175] and another Group of Governmental Experts[176] will address the beforementioned challenges. Both groups began their work in December 2019, and the OEWG is expected to report back to the General Assembly in the fall of 2020, whereas the new GGE is to submit its final report in 2021.[177]

2.4 "Below the threshold" cyber operations distinguished and defined

First and foremost, it is paramount to underline the fact that no general prohibition of cyber operations exists in international law.[178] There is no legally binding definition of the term and no universally agreed upon definition exists. Furthermore, there has been a rather small amount of conversation on the permissibility of cyber operations in general or specifically regarding the means and methods used to conduct cyber operations.[179] However, the term cyber operation has become a common denominator for "activities in cyberspace, undertaken with the aim of achieving objectives in or through this digital domain … in a great variety of situations, by a diversity of actors and, quite obviously for various reasons."[180]

As can be denoted from the previous quote, cyber operations do not only occur in cyberspace, but also through it. Accordingly, a similar definition is found in Tallinn Manual 2.0, where the manual defines cyber operations as "the employment of cyber capabilities to achieve objectives in or through cyberspace."[181] The Manual also refers to cyber operations as "cyber activity", which in turn is defined as "any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure."[182] Conversely, "cyber attack" is probably the most frequently used term when describing malicious cyber activities. Tallinn Manual 2.0 defines a cyber attack as

[175] UN Doc. A/RES/73/27 (11 December 2018). It is also noteworthy to mention that the resolution underscored the fact that "while States have primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations." Ibid, p. 5. Furthermore, the OEWG is open to all UN member states.
[176] UN Doc. A/RES/73/266 (2 January 2019).
[177] UNODA, 'Fact Sheet on Developments in the Field of Information and Telecommunications in the Context of International Security', available at https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.
[178] Delerue (n 48), p. 193.
[179] Tikk (n 92), p. 14.
[180] Ducheine, Pijpers (n 106), p. 7.
[181] Tallinn Manual 2.0, p. 564.
[182] Ibid.

"cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[183] NATO, on the other hand, identifies "computer network attacks" (CAN) as "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself, … [a] computer network attack is a type of cyber attack."[184]

The most common cyber operations are so called Distributed Denial of Service attacks (DDoS) and semantic attacks.[185] DDoS attacks are deliberate attempts to disrupt or degrade a network or service.[186] The attacks flood a network thus preventing legitimate data traffic, often resulting in a temporary shutdown.[187] Typically, the attacker will use a virus to take over hundreds or thousands of computers in order to form a botnet of zombie computers.[188] In the 2007, Estonia was hit by a large scale DDoS attack, targeting *inter alia* government websites, financial institutions, and media outlets.[189] At least a *million* computers were reported to have been used to launch the attacks.[190] The attacks, widely reported in the media as "cyber war",[191] were conducted in response to the Estonian government's decision to relocate a Soviet-era statute from the central of its capital,

[183] Tallinn Manual 2.0, rule 92 – Definition of cyber attack, p. 415.
[184] NATO Glossary of Terms and Definitions (AAP-07, Edition 2019), p. 30, available at https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF. However, NATO leaders have agreed that cyber attacks are a threat to the alliance, but a "lack of unity creates problems for the public in understanding the threat and for governments in responding to them." See Christopher Woody, 'NATO leaders are worried about cyberattacks, but it's not clear they all agree on what that means', 2 October 2018, Business Insider, available at https://www.businessinsider.com/nato-leaders-agree-cyberattacks-are-threat-but-cant-agree-definition-2018-10?r=US&IR=T.
[185] Hathaway, Crootof (n 34), p. 837.
[186] Seth Djane Kotey, Eric Tutu Tchao, James Dzisi Gadze, 'On Distributed Denial of Service Current Defense Schemes' (2019), available at https://www.mdpi.com/2227-7080/7/1/19/htm.
[187] Peter Margules, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2015), p. 6. The Tallinn Manual 2.0 defines a DDoS attack as "A technique that employs two or more computers, such as the bots of a botnet, to achieve a denial of service from a single or multiple targets." Tallinn Manual 2.0, p. 565.
[188] Margules (n 187), p. 6.
[189] It is virtually impossible to engage in a cyber related debate without mentioning the infamous DDoS attacks against Estonia. It is thus unsurprising how the Tallinn Manuals have gotten their names.
[190] Ian Traynor, 'Web attackers used a million computers, says Estonia', 18 May 2007, The Guardian, https://www.theguardian.com/technology/2007/may/18/news.russia. (Emphasis added).
[191] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', 17 May 2007, The Guardian, https://www.theguardian.com/world/2007/may/17/topstories3.russia. The former Estonian president, Toomas Hendrik Ilves, also described the DDoS attacks as 'Web War One', see https://vp2006-2016.president.ee/en/official-duties/speeches/8003-president-toomas-hendrik-ilves-keynote-speech-at-the-3rd-annual-billington-cybersecurity-summit-washington-dc-september-27th-2012/index.html

Tallinn, to a nearby military cemetery.[192] The Estonian government publicly accused the Russian government for the attacks, stating that "IP addresses have helped to identify that the… attacks … have originated from specific computers and persons in Russian government agencies, including the administration of the President of the Russian Federation."[193] However, despite the initial allegations, Russia repeatedly denied any responsibility[194] and ultimately, the Estonian government concluded that there were insufficient evidence of a Russian governmental role.[195] Therefore, the attacks were never legally attributed to Russia and in the end, they were dealt with as a domestic criminal matter.[196]

The attacks did not *per se* cause any physical damage but produced a vast societal disruption and the economic impact was estimated to be several million euros.[197] However, in both scale and duration, the DDoS attacks against Estonia were up until then unparalleled, and it became clear that the international community was ill prepared to handle this new domain of interstate conflict.[198] The attacks further unveiled the difficulties inherent with the attribution of conduct in cyberspace, as well as the challenges in holding states responsible for malicious cyber activities originating from their sovereign territories. The DDoS attacks against Estonia thus served as a catalyst for the important discussion on issues relating to the regulation of cyberspace,[199] contributing to the birth of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the Tallinn Manual process.[200]

---

[192] Schmitt (n 65), p. 242; Steven Lee Myers, 'Estonia removes Soviet-era war memorial after a night of violence', 27 April, The New York Times, https://perma.cc/CR6F-N33V.
[193] Declaration of the Minister of Foreign Affairs of the Republic of Estonia, 1 May 2007, https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia.
[194] Samuli Haataja, 'The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach' (2017), p. 3.
[195] Sputnik News, 'Estonia has no evidence of Kremlin involvement in cyber attacks', 6 September 2007, https://sputniknews.com/world/2007090676959190/;
[196] Only one person was convicted for taking part in the attacks, and was subsequently fined, see BBC News, 'Estonia fines man for 'cyber war', 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.
[197] Haataja (n 194), p. 3. Some reports have estimated that economic loss would have amounted to anywhere between 27 to 40 million US dollars. Ibid.
[198] Schmitt (n 65), p. 242.
[199] Broeders, van den Berg (n 39) p. 21.
[200] Tallinn Manual 2.0, p. xxii, Foreword by Toomas Hendrik Ilves, former president of the Republic of Estonia.

Semantic attacks use "malicious computer code or malware such as 'worms, viruses and Trojan horses' to compromise operating systems."[201] These types of attacks "do not destroy the computer's operating system; instead, they operate more subtly, changing the data generated by monitoring software while maintaining the illusion that the network is fully functional."[202] Further, since the machine's operator does not display the correct data, the machine continues to function even though it should have stopped running and therefore leads to self-destruction.[203] In July 2010, the Stuxnet (also known as Olympic Games), a 500-kilobyte computer worm,[204] was detected by a Belarusian cyber security company, VirusBlokAda, and it was discovered to have infected thousands of SCADA-systems around the world.[205] Despite having spread to several different countries, 58.31 % of infected hosts were located in Iran.[206] In other words, the Stuxnet was specifically used to target Iranian nuclear facilities and reportedly destroying numerous centrifuges in Iran's Natanz uranium enrichment facility.[207] In the months that followed it became clear that the Stuxnet virus was far more sophisticated than any other previously seen.[208] The research into Stuxnet revealed that it was launched already in June 2009, and a total of three different versions had been released prior to the reveal.[209] Most importantly, the Stuxnet represents the first time the world "had seen digital code in the wild being used to physically destroy something in the real world."[210] Iran has not publicly attributed the

[201] Margules (n 187), p. 6.
[202] Ibid, p. 7.
[203] Ibid.
[204] A worm is defined as "a virus-like program that seeks out other connected hosts in a computer network and, by exploiting a vulnerability transfers itself to them." A Dictionary of Computer Science (7 ed.) (2016), Oxford University Press, p. 607, available at https://www.oxfordreference.com/view/10.1093/acref/9780199688975.001.0001/acref-9780199688975-e-5858?rskey=VpEjVB&result=6417
[205] Duncan B. Hollis, 'Could Deploying Stuxnet be a War Crime?', 25 January 2011, Opinio Juris, http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/.
[206] Approximately 115 countries were infected, with Indonesia (17.83%) and India (9.96%) being the worst countries affected after Iran. https://www.statista.com/statistics/271110/stuxnet-infected-hosts-by-country/.
[207] McAfee, 'What Is Stuxnet?' https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.
[208] Lawrence J. Trautman, Peter C. Ormerod, 'Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things' (2018), p. 787.
[209] Ibid.
[210] Kim Zetter, 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History' (2011), available at https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Stuxnet virus to any state, but it is widely suspected that it was a joint operation launched by the United States and Israel.[211]

Since the DDoS attacks against Estonia and the Stuxnet virus, several other costly and intrusive state cyber operations have taken place,[212] including the 2012 Iranian-linked Shamoon malware attack against Saudi Arabia,[213] the 2014 Sony hack,[214] the 2015 Russian-linked attack on the Ukrainian power grid,[215] and the 2016 DNC hack.[216] More recent cyber operations include the 2017 WannaCry ransomware attack[217] and NotPetya.[218] In order to further illustrate the implications of malicious cyber operations, the WannaCry ransomware attack will be presented and analyzed in depth below.

[211] Ellen Nakashima, Joby Warrick, 'Stuxnet was work of U.S. and Israeli experts, officials say', 2 June 2012, The Washington Post, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html; David E. Sanger, 'Obama Ordered Sped Up Wave of Cyberattacks Against Iran', 1 June 2012, The New York Times, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; Katharina Ziolkowski, 'Stuxnet – Legal Considerations' (2012).

[212] Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace' (2018), p. 575.

[213] Salem Alelyani, Harnish Kumar G. R., 'Overview of Cyberattack on Saudi Organizations' (2018).

[214] Clare Sullivan, 'The 2014 Sony Hack and The Role of International Law' 21 July 2016, available at https://jnslp.com/2016/07/21/2014-sony-hack-role-international-law/.

[215] Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (2016), available at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[216] David E. Sanger, Nick Corosaniti, 'D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump', 14 June 2016, The New York Times, https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

[217] Michael Schmitt, Sean Fahey, 'WannaCry and the International Law of Cyberspace', 22 December2017, Just Security, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/.

[218] Michael Schmitt, Jeffrey Biller, 'The NotPetya Cyber Operation as a Case Study of International Law', 11 July 2017, EJIL: Talk! https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/-

3. Internationally wrongful acts in cyberspace

3.1 Invoking state responsibility

In May 2017, the NHS (National Health Service) services across the United Kingdom were hit by a large-scale global ransomware[219] attack WannaCry, as staff at hospitals and other medical facilities were blocked access to patient data, causing ambulances and emergency rooms to divert patients.[220] Moreover, thousands of operations and appointments were cancelled, and a ransom demand in the cryptocurrency Bitcoin was set.[221] While the United Kingdom was particularly effected,[222] it was neither the specific nor sole target – WannaCry had an unprecedented global reach, crippling an estimated 200,000 computers in at least 150 countries.[223] To illustrate the outreach, over 1,000 computers of the Russian Interior Ministry were affected by the ransomware, as was the U.S. Delivery company FedEx, German railways, Chinese universities, and some Renault car factories in France were forced to halt production.[224] Consequently, according to Europol, the WannaCry cyber attack constituted the "largest ransomware attack observed in history".[225] Furthermore, the WannaCry was characterized as "a careless and reckless attack. It affected individuals, industry, governments. And the consequences were beyond economic. The computers affected badly in the UK and their healthcare system put lives

[219] Ransomware is form of malware used to lock, limit, and prevent a user from accessing data in their computer system, therefore pressing the victim to pay ransom in order to regain control of their data. See European Union Agency for Cybersecurity (ENISA), Glossary, 'Ransomware', https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware.

[220] BBC News, 'NHS cyber-attack: GPs and hospitals hit by ransomware', 13 May 2017, https://www.bbc.com/news/health-39899646; Russel Goldman, 'What We Know and Don't Know About the International Cyberattack', 12 May 2017, New York Times, https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html.

[221] United Kingdom, Department of Health, Report by the Comptroller and Auditor General, 'Investigation: WannaCry cyber attack and the NHS', 28 April 2018, available at https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. According to the report, no ransom demands were paid.

[222] Matthew Field, 'WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled', 11 October 2018, The Daily Telegraph, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[223] Reuters, 'Cyber attack hits 200,000 in at least 150 countries: Europol'

[224] Michael Schmitt, Sean Fahey, 'WannaCry and the International Law of Cyberspace', 22 December 2017, Just Security, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/; BBC, 'Ransomware cyber-attack: Who has been hardest hit?'. 15 May 2017, https://www.bbc.com/news/world-39919249. In specific, the WannaCry ransomware attack targeted and exploited vulnerabilities in systems operating older versions of Microsoft Windows.

[225] BBC, 'NHS cyber-attack: No 'second spike' but disruption continues', 15 May 2017, https://www.bbc.com/news/uk-39918426.

at risk, not just money."[226] Conversely, a cyber operation that compromises hospital files, company data or university computers certainly does not amount to an act of war or a potential use of force but is nonetheless of serious concern.[227]

As has become apparent, it is recognized that states carry out malicious cyber operations against each other in or through cyberspace.[228] Cyber operations that, for instance, destroy data and sabotage cyberinfrastructure are on the rise,[229] and some states have even publicly expressed a strategic interest in conducting such cyber activity,[230] but are paradoxically unwilling to be identified as the perpetrator of a hostile cyber operation.[231] In other words, some states utilize cyber tools to conduct cyber operations with impunity, "knowing (or at least strongly suspecting) that their digital attacks will not prompt a response, certainly not a kinetic response."[232] Up to the present, not a single state has claimed responsibility for launching or conducting malicious cyber operations, nor attempted to publicly justify them, and it seems to denote a willingness of states to operate "below the radar", as well as signalling an uncertainty regarding the lawfulness of their own conduct under extant international law.[233] Accordingly, it can be held that states regularly avoid responsibility for their malicious cyber activities.[234] For instance, Russia has been accused of having conducted several cyber operations against other states' critical infrastructure but dismisses any accusations of wrongdoing and demands the proof of hard evidence.[235]

---

[226] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, December 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacrymalware-attack-to-north-korea-121917/.
[227] Crootof (n 212), p. 596.
[228] Michael N. Schmitt, Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014), p. 55
[229] Tikk (n 92), p. 11.
[230] See e.g. The Netherlands, 'Defence Cyber Strategy' (2015), where the Netherlands Defence organisation states that it will develop "offensive cyber assets and … cyber intelligence assets for tactical use." Available at https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy. Correspondingly, the United Kingdom has openly declared its intentions to become "a world leader in offensive cyber capability", see United Kingdom, 'National Cyber Security Strategy 2016-2021', p. 51, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Schmitt, Vihul (n 228), p. 55.
[231] Schmitt, Vihul (n 228), p. 55
[232] Banks (n 43), p. 191.
[233] Efrony, Shany (n 102), pp. 594, 597.
[234] Jensen, Watts (n 1), p. 1559.
[235] Piret Pernik, 'Responding to "the Most Destructive and Costly Cyberattack in History"', 23 February, https://icds.ee/responding-to-the-most-destructive-and-costly-cyberattack-in-history/. For instance, in relation to the DNC Hack, a spokesman for the Russian president claimed that the U.S. should "either stop

In the case of WannaCry, the United States publicly attributed the malevolent ransomware attack to North Korea.[236] However, the attack was never characterized under international law,[237] and no measures of accountability were taken against Pyongyang, either by the United States or by the hardest hit nation the United Kingdom.[238] Instead the attack was referred to as a "criminal use of cyberspace."[239] North Korea responded to the attribution claims, calling the accusations "groundless speculation" and "a wicked attempt to tighten international sanctions on the country."[240] The WannaCry incident, like other "below the threshold" cyber operations, thus warrants the question of how states can be held responsible for malicious cyber operations. The attack illustrates the complexity of applying international law to ambiguous and abstruse cyber scenarios and the incident undoubtedly also raises questions regarding state obligations with respect to cyber activities.[241]

In the physical world, whenever an internationally wrongful act occurs for which no state has claimed responsibility, the injured state must endeavor to establish international responsibility for that act in order to be able to respond to or make demands against the responsible state from whose territory it originated.[242] While the general applicability of the customary rules of state responsibility to cyberspace is not contested, many specific aspects remain problematic. Cyberspace and cyber operations challenge the traditional

talking about that or produce some proof at last. Otherwise it all begins to look unseemly." Laura Smith-Park, 'Russia challenges US to prove campaign hacking claims or shut up', 16 December 2016, CNN, https://edition.cnn.com/2016/12/16/europe/russia-us-hacking-claims-peskov/index.html.

[236] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, December 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacrymalware-attack-to-north-korea-121917/. The United States stated that: "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.".

[237] Delerue (n 48), p. 230.

[238] Michael J. Adams, Megan Reiss, 'How Should International Law Treat Cyberattacks like WannaCry?', 22 December 2017, Lawfare, https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry.

[239] United Kingdom, Statement of Foreign Minister, Lord Ahmad, 'Foreign Office Minister condemns North Korea actor for WannaCry attacks', 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

[240] BBC, 'North Korea calls UK WannaCry accusations 'wicked'', 31 October 2017, https://www.bbc.com/news/world-asia-41816958.

[241] Jensen (n 3), p. 1.

[242] Efrony, Shany (n 102), p. 632.

framework of international state responsibility in both a technical and legal manner, and more specifically cyber attribution has been described as "more art than science."[243] The technical challenges of identifying the responsible entity behind cyber operations has also led to an impression that states can act with impunity, as cyberspace offers nations "a covert means of pursuing national security objectives."[244] An example of the latter is the 2018 Winter Olympic Games in PyeongChang, South Korea, where several hundred computers belonging to South Korean governmental authorities were hacked moments before the beginning of the Opening Ceremony.[245] Given South Korea's turbulent history and geopolitical conflicts with its Northern neighbor, North Korea was quickly pointed out as a suspect.[246] However, by using North Korean IP addresses (so-called false flag operation), the cyber operation was in fact conducted by Russia, seemingly as retaliation against the International Olympic Committee for the banning of Russian athletes from the Winter Games due to previous doping violations.[247]

In other words, anonymity, together with the classified nature of state cyber operations represent a clear obstacle in allocating state responsibility,[248] and further challenge the identification of current state practice and *opinio juris* regarding state activity in cyberspace. It has been observed, that the legality of state cyber operations has not extensively been questioned, as a significant amount of the known cyber operations have been conducted in a so called grey zone of international law.[249] Moreover, it has also been claimed that the Tallinn Manual 2.0 provides victim states with extremely insufficient advice on how to react to malicious cyber operations, and thus leaving them with a very

[243] Banks (n 50), p. 1493.
[244] Schmitt, Vihul (n 228), p. 55
[245] BBC, 'Winter Olympics hit by cyber-attack', 12 February 2018, https://www.bbc.com/news/technology-43030673.
[246] Andy Greenberg, 'The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History', 17 October 2019, Wired, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.
[247] Ellen Nakashima, 'Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say', 25 February 2018, the Washington Post, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.
[248] François Delerue, 'Attribution to State of Cyber Operations Conducted by Non-State Actors' (2019), p. 235.
[249] Delerue (n 48), p. 197; See generally Michael Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017).

limited amount of legal response options.[250] The surrounding debate regarding cyber attribution and possible state responses to malicious cyber operations will be discussed in greater detail in the next chapter. Subsequently, this thesis now turns to examine the paradigms of state responsibility and how they apply to malicious interstate cyber operations. The later subchapters focus on how cyber operations can violate the principles of sovereignty and non-intervention in the external or internal affairs of a state, thus amounting to an internationally wrongful act.

3.2 Elements of state responsibility

States are responsible for their internationally wrongful acts pursuant to the law of state responsibility.[251] In other words, the law of state responsibility amounts to a "general law of wrongs"[252] and is viewed as a cardinal institution of public international law.[253] As the principal bearers of international obligations,[254] every violation by a state of its international obligations entails its responsibility.[255] Strictly speaking, when a state commits an internationally wrongful act against another state, multiple states, or the international community as a whole,[256] international responsibility arises. Accordingly, in order to safeguard the integrity of the international legal order and to offer protection to the victim of the unlawful act (the injured state), the breach cannot be left without legal repercussions. Subsequently, state responsibility aims at answering three questions:

---

[250] Efrony, Shany (n 102), p. 593.
[251] Draft Articles, art. 1 "Every internationally wrongful act of a State entails the international responsibility of that State"; UN GGE Report, para. 23; UN GGE Report, para. 28(f); Tallinn Manual 2.0, p. 84.
[252] James Crawford, Simon Olleson, 'The Character and Forms of International Responsibility' (2018), p. 449.
[253] James Crawford, State Responsibility, Max Planck Encyclopedia of Public International Law [MEPIL], September 2006, Oxford Public International Law.
[254] Ibid.
[255] "The general principles of International Law concerning State responsibility are equally applicable in the case of breach of treaty obligation, since in the international law field there is no distinction between contractual and tortious responsibility, so that any violation by a State of any obligation, of whatever origin, gives rise to State responsibility." Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 2986 between the two States and which related to the problems arising from the *Rainbow Warrior* affair, UNRIAA, vol. XX, p. 215 (1990), para. 75; Draft Articles, Commentary, ch. 1, cm. 2, p. 33.
[256] Draft Articles, art. 33: "The obligations of the responsible State … may be owed to another State, to several States, or to the international community as a whole, depending in particular on the character and content of the international obligation and on the circumstances of the breach."

1) Has a breach of an international legal obligation by a state occurred?
2) What are the legal consequences of such a breach?
3) What are the permissible responses of such a violation, and who may respond to it?

The International Court of Justice (ICJ) has confirmed the customary nature of the principle of state responsibility in several of its judgments.[257] Furthermore, the customary international law of state responsibility is in greatly reflected and crystalized in the work of the International Law Commission (ILC) and its Draft Articles on Responsibility of States for Internationally Wrongful Acts.[258] The Draft Articles are the result of a drafting process lasting over half a century under the direction and guidance of five special rapporteurs.[259] The Draft Articles have since their completion in 2001 been commended to UN member states by the UN General Assembly and have frequently been cited by international courts, tribunals and other bodies.[260] Additionally, the Tallinn Manual 2.0 also follows the Draft Articles, and states that the rules are "based on customary international law of State responsibility, which is largely reflected in the International Law Commission's Articles on State Responsibility and upon which the Rules …rely in

[257] See e.g., Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) ICJ Reports 1980; Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America), paras. 283, 292. The Permanent Court of Justice also confirmed the same principle, see e.g. Phosphates in Morocco (Italy v. France), 1938, P.C.I.J "This act being attributable to the State and described as contrary to the treaty right of another State, international responsibility would be established immediately as between the two States."; Case of the S.S. "Wimbledon" (United Kingdom, France, Italy & Japan v. Germany), 1923, para. 30

[258] The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission, 53rd session, (Apr. 23-June 1,July 2-Aug. 10, 2001), General Assembly Official Records, 56th session, supp. no. 10, UN Doc. A/56/10.

[259] James Crawford, State Responsibility, Max Planck Encyclopedia of Public International Law [MPEPIL], September 2006, Oxford Public International Law. Dionisio Anzilotti's works *Teoria generale della responsabilità dello Stato nel diritto internazionale* (1902) and *La responsabilité internationale des Etats* (1906) are considered to be leading contributions to the branch of international law of state responsibility before the First World War. See Georg Nolte, 'From Dionisio Anzilotti to Roberto Ago: The Classical International Law of State Responsibility and the Traditional Primacy of a Bilateral Conception of Inter-state Relations' (2002), p. 1084. However, the work on state responsibility in the ILC began in 1956, under Special Rapporteur García Amador, followed by Roberto Ago, Willem Riphagen, Gaetano Arangio-Ruiz, and culminated under James Crawford. For further information on the work of the ILC, see 'Analytical Guide to the Work of the International Law Commission', available at https://legal.un.org/ilc/guide/9_6.shtml. See also James Crawford, 'The International Law Commission's Articles on State Responsibility: Past and Future', UN Audiovisual Library, lecture available at https://legal.un.org/avl/ls/Crawford_S.html.

[260] "By 2012, the Articles and the accompanying commentary had been cited 154 times by international courts, tribunals and other bodies." Tallinn Manual 2.0, p.79, note 112. See also Banks (n 50), p. 1495.

great part."[261] In 2020, the Second Pre-draft of the OEWG also reiterated the that "under customary international law, the responsibilities of States with regard to internationally wrongful acts extend to their use of ICTs."[262]

The Draft Articles set forth two criteria, one objective and subjective element, as a precondition for finding a state responsible for an internationally wrongful act:

> 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.[263]

Firstly, the internationally wrongful act must be attributable to a state and, secondly, the conduct must constitute a breach of an international obligation owed to the victim state at the time.[264] This was echoed in the Tallinn Manual 2.0, as it reaffirms that "[a] State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[265]

In light of the above, however, the law of state responsibility has been regarded as one of the most complex areas of public international law, largely due to its theoretical nature, seeing at it "tends to be a complex field in which principles are articulated at a level of abstraction that obfuscated their theoretical underpinning."[266] Accordingly, the law of state responsibility is frustrated in the context of cyberspace and malicious cyber operations.[267] First and foremost, internationally wrongful cyber acts merit a thorough discussion. In other words, under what circumstances and what type of cyber operations constitute an internationally wrongful act pursuant to article 1 of the Draft Articles? That said, as it would be difficult to classify all the possible international law norms that cyber

[261] Tallinn Manual 2.0, p. 79.
[262] Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[263] Draft Articles, art. 2.
[264] See e.g. Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) ICJ Reports 1980.
[265] Tallinn Manual 2.0, rule 14 – Internationally wrongful cyber acts, p. 84.
[266] René Provost (ed), 'State Responsibility in International Law' (2002), p. 14
[267] Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace' (2017), p. 645.

operations could potentially violate, the choice of focus in this thesis is on the principles of state sovereignty and non-intervention.[268]

The international legal order consists of international legal obligations that are reciprocal in nature. Consequently, acts in violation of such obligations owed to another state may cause injury or damage to the state to which they are owed to. As an initial matter, a general prohibition of cyber operations does not exist in international law, nor does every malicious cyber activity engage a state for the purpose of state responsibility.[269] While cyber operations are not unlawful *per se*, they can constitute hostile or unfriendly acts, defined as "conduct (act or omission) of a subject of international law which inflicts a disadvantage, disregard or discourtesy on another subject of international law without violating any legal norm."[270] Such conduct could therefore be considered as a breach of good relations, hence inflaming interstate relations without resulting in any legal consequences.[271] Unfriendly acts are not prohibited under international law[272] but states should "refrain from any action which may aggravate the situation so as to endanger the maintenance of international peace and security, and shall act in accordance with the purposes and principles of the United Nations."[273] However, states have no legal obligation to abstain from such conduct. In other words, certain cyber activity against another state may be regarded as injurious or unfriendly, but if it is not in breach of international law obligations, states legal responsibility cannot be invoked.[274] Tallinn Manual 2.0 offers an example - state A's suspension of e-commerce with state B (e.g. through the blocking of specific commercial websites), might be regarded as unfriendly and potentially leading to economic loss, but generally does not entail a breach of an international obligation.[275]

---

[268] "Especially prominent among the relevant customary norms, breaches of which constitute internationally wrongful acts, are respect for sovereignty […] [and] the prohibition of intervention […]." Tallinn Manual 2.0, p. 85.
[269] Delerue (n 48), p. 194.
[270] Dagmar Richter, 'Unfriendly Act', Max Planck Encyclopedia of Public International Law [MPEPIL], https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e423; Delerue (n 48), p. 194.
[271] Delerue (n 48), p. 194.
[272] See Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Untied States of America) [1986] ICJ Reports 14 136-137, para. 273.
[273] Declaration on Principles of International Law concerning Friendly Relation and Cooperation among States in Accordance with the Charter of the United Nations', UNGA Res 2625 (XXV), 24 October 1970.
[274] Draft Articles, General Commentary, para. 4; Tallinn Manual 2.0, p. 86.
[275] Tallinn Manual 2.0, p. 86.

The mere fact that a cyber operation occurs in or through cyberspace does not automatically render it unlawful, an example of the latter being cyber espionage, which Tallinn Manual 2.0 defines as "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information"[276] The International Group of Experts agreed that customary international law does not prohibit espionage *per se*.[277] While not unlawful standing alone, cyber espionage may nonetheless constitute "an integral and indispensable component of an operation that violates international law."[278] The question at hand is therefore what type of activities constitute international wrongful acts and under which circumstances? More specifically, what is an internationally wrongful act in the cyber context?

> An internationally wrongful act of a State may consist in one or more actions or omissions or a combination of both. Whether there has been an internationally wrongful act depends, first, on the requirements of the obligation which is said to have been breached and, secondly, on the framework conditions for such an act …[279]

What constitutes an internationally wrongful act is determined by what primary international obligation has been violated, as primary rules set forth the international law obligations and violations thereof result in state responsibility.[280] Secondary rules lay down the general conditions under which a state is entitled to respond to a violation of an international obligation.[281] In other words, the essence of an internationally wrongful act lies "in the non-conformity of the State's actual conduct with the conduct it ought to have adopted in order to comply with a particular international obligation."[282] In most circumstances, this would seem rather straightforward, for instance if state A's military forces use force against state B, the former would be violating the prohibition on the use of force enshrined in Article 2 (4) of the UN Charter.[283] Accordingly, it must be kept in mind that the existing rules of state responsibility were established during a pre-cyber era where it was relatively uncomplicated to establish an occurrence of an internationally

[276] Tallinn Manual 2.0, p. 168.
[277] Tallinn Manual 2.0, p. 169.
[278] Tallinn Manual 2.0, p. 171. However, espionage is penalized by a majority of states under their respective domestic law. Delerue (n 48), p. 194.
[279] Draft Articles, art. 1, para. 1 of the commentary.
[280] Draft Articles, General Commentary (1), p. 31.
[281] Draft Articles, General Commentary (1) (h), p. 31.
[282] Draft Articles, commentary, ch. 3, cm. 3.
[283] UN Charter, art. 2 (4).

wrongful act, as can be illustrated with the example of prohibited uses of force. In other words, establishing the occurrence of an internationally wrongful act in cyberspace poses a whole array of unprecedented difficulties.

An internationally wrongful act can be an act or an omission. An internationally wrongful act on behalf of a state can for instance be non-compliance with a treaty obligation or an illegal use of force, whereas an omission can consist of a state remaining passive in fulfilling its legal obligations.[284] However, determining when an omission has occurred is not forthright, as it may be difficult to prove that a state was not aware of a duty owed to another state. In the cyber context, an internationally wrongful act may consist of a state actually conducting a malicious cyber operation or a state, having knowledge of such malicious activity, fails to stop it. Furthermore, the causation of damage is not a *conditio sine que non* for the characterization of a cyber operation as unlawful (unless the damage or injury is an element of breach of the primary rule) and therefore an internationally wrongful act.[285] The geographic location from which a cyber operation is launched is not determinative when determining state responsibility, as they may be conducted from the a responsible state's own territory, from within the victim state's territory, a third state's territory, the high seas, international airspace or outer space.[286]

As discussed above, for a state to be held responsible for a cyber operation, that cyber operation must be attributable to that state and in violation of international law, and therefore amounting to an internationally wrongful act. While a general prohibition of cyber operations is indeed conspicuous by its absence, the launching of cyber operations may nonetheless violate specific norms of international law.[287] Put differently, cyber operations are subject to rules from various international legal regimes,[288] and it has been

[284] "Cases in which international responsibility has been invoked on the basis of an omission are at least as numerous as those based on positive acts, and no difference in principle exists between the two." Draft Articles, art. 2, para. 4 of the commentary, p. 35.
[285] Tallinn Manual 2.0, p. 86.
[286] Tallinn Manual 2.0, p. 87. However, the Manual does state that certain internationally wrongful acts are in fact geographically dependent, especially in relation to outer space, international airspace and the high seas. For instance, in order for a breach of the innocent passage regime to occur, the vessel used to conduct a cyber operation needs to be present within the victim state's territorial waters. Tallinn Manual 2.0, p. 87.
[287] Delerue (n 48), p. 183.
[288] Schmitt (n 65), p. 256. For instance, "cyber espionage may implicate the international human right of privacy, while a state's imposition of controls on cyber activities can implicate the right to freedom of expression." (Ibid).

held that the most likely breach is a "violation of the sovereignty of the state in which, or into which, another state's cyber operations are conducted."[289]

3.3 Sovereignty in cyberspace

Sovereignty is undeniably a complicated subject of debate and has become a matter of concern especially within the cyber domain. More specifically, the question of how the principle of sovereignty governs state cyber activity has become the number one topic of discussion for legal scholars.[290] As previously established, cyberspace is a manmade, fictional territory that is based on real and tangible infrastructures. Moreover, the computer network and the components used to launch malicious cyber operations are located in the sovereign territory of a state. Correspondingly, the users of cyberspace will also be physically present within a certain jurisdiction at any given moment. Therefore, this subchapter seeks to analyse how a remote[291] state cyber operations can violate the principle of state sovereignty. Further, the purpose of this subchapter is also to shed some light on the debate whether sovereignty constitutes a standalone rule of international law.

Before probing the waters of when a cyber operation is in breach of sovereignty, the thesis turns to briefly analysing the general principles of sovereignty and how they are applicable to the cyber context. As a starting point, sovereignty signifies "independence in regard to a portion of the globe [and] is the right to exercise therein, to the exclusion on any other State, the functions of a State."[292] The definition sets forth two of the core aspects of sovereignty – territorial integrity and state functions. In other words, based on the notion of sovereignty, in the absence of a legal prohibition, states enjoy freedom of action.[293]

---

[289] Schmitt (n 65), p. 257.
[290] NATO CCDCOE, 11th International Conference on Cyber Conflict (CyCon 2019), Michael Schmitt 'Sovereignty and Cyber Operations', video available at https://www.youtube.com/watch?v=u0Ikg8RjITY&t=1241s.
[291] As state actors are rarely physically present on the territory of the state against which a cyber operation may be conducted, the underlying understanding of the usage of 'cyber operation' throughout will denote that the operation is launched from outside the territory of the injured state.
[292] Island of Palmas (United States v. Netherlands) Permanent Court of Arbitration (PCA), 4 April 1928.
[293] Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' (2013), p. 135.

The principles of state sovereignty and jurisdiction – despite being two distinct concepts – are used interchangeably, often leading to confusion.[294] The former reflects a state's supreme legal authority within a specific territory, whereas the latter refers to the power of the state to define and enforce rights and duties, and to control the conduct of juridical and natural persons.[295] The principle of sovereignty is a long-established concept, dating back to the Peace of Westphalia in 1648.[296] Sovereignty is a foundational principle upon which must of the rest of international law is built[297] and several notions derive from the principle of sovereignty, *inter alia*, the prohibition of non-intervention, prohibition against the use of force, and due diligence.[298] Sovereignty indicates the equality of states, and the principle is enshrined in the UN Charter.[299]

Today, states regularly exercise legal authority over actors and activities in cyberspace based on their borders, in other words "based on the physical location of the network(s) or server(s) employed, or the physical location where the effects of such activity occur."[300] In the context of cyberspace, territory is to be seen as the territory connected to the physical, tangible aspects of cyberspace, for instance the computer used and the individual behind the deployment of the cyber operation. Accordingly, the Tallinn Manual 2.0 provides: "A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[301]

The quote above illustrates the internal aspect of sovereignty. In contrast, the external component of sovereignty, deriving from the sovereign equality of states,[302] denotes a state's right to engage in international relations.[303] For instance, a state is free to decide

[294] Delerue (n 48), p. 208.
[295] Ibid.
[296] Bardo Fassbender, 'Westphalia, Peace of (1648), Max Planck Encyclopedias of International Law, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e739.
[297] ICJ *Nicaragua*, para. 263: "the fundamental principle of State sovereignty, on which the whole of international law rests".
[298] Michael Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017), p. 4.
[299] UN Charter, art. 2(1): "The Organization is based on the principle of the sovereign equality of all its Members."
[300] Hollis (n 134), p. 6.
[301] Tallinn Manual 2.0, Rule 2 – Internal sovereignty, p. 13.
[302] The principle of sovereign equality of states was also reaffirmed in UN GGE 2015 report, paras. 26, 28 (b).
[303] Tallinn Manual 2.0, p. 16.

whether it will opt into a specific treaty governing cyber activities.[304] However, while it is accepted that states have the sovereign right to control movement within and across their borders, the issue becomes more problematic in cyberspace where boundaries are not defined, hence making it difficult to identify whether a state border is crossed.[305] Furthermore, while cyber operations have a tangible aspect, for example computer hardware, interactions in cyberspace "also have a 'virtual' dimension, through the transmission of data, signalling, and sending of content between physical devices."[306] Accordingly, it stands to reason that there are no visible or identifiable borders in cyberspace, and that data and information are constantly travelling in between various servers, thus in fact crossing physical borders.[307] That said, it has been suggested that the Westphalian form of sovereignty is completely irrelevant in the cyber context.[308] It has further been questioned whether the maintenance of territorial and conceptual borders associated with national sovereignty is compatible with the asymmetric and borderless cyberspace.[309]

Notwithstanding the foregoing, the applicability of sovereignty to state cyber activities is beyond question,[310] and while cyberspace certainly differs from the physical domains, there is no reason to claim that it should be governed by different legal standards.[311] However, while the existence of a principle of sovereignty in cyberspace is not contested, the disagreement lies in whether sovereignty constitutes a primary rule of international law, for only the breach of an obligation contained in a primary rule of international law qualifies as an internationally wrongful act.[312] Considering the above, the United States and the United Kingdom have expressed a view according to which sovereignty cannot be violated in cyberspace, and these views will be discussed in turn below. Conversely, on other end of the spectrum, Russia and China are ardently convinced of the binding

[304] Tallinn Manual 2.0, p. 17.
[305] Adrian Venables, 'Establishing Cyber Sovereignty – Russia Follows China's Example', 20 March 2019, https://icds.ee/establishing-cyber-sovereignty-russia-follows-chinas-example/.
[306] Moynihan (n 4), p. 14.
[307] Delerue (n 48), p. 222.
[308] Cynthia E. Ayers, 'Rethinking Sovereignty in The Context of Cyberspace' (2016), p. ix.
[309] Ibid.
[310] Gary P. Corn, Robert Taylor, 'Sovereignty in The Age of Cyber' (2017), p. 207.
[311] Henriksen (n 18), p. 331; UN GGE consensus reports of 2013 and 2015.
[312] Michael N. Schmitt, Liis Vihul, 'Sovereignty In Cyberspace: *Lex Lata Vel Non*' (2017), p. 213.

nature of sovereignty and have tried to align cyberspace with territorial boundaries.[313] In 2016, both countries signed a Joint Statement on Cooperation in Information Space Development,[314] which specifically provides that the states "jointly advocate respect to and oppose infringements on every country's sovereignty in information space."[315] Furthermore, China – allegedly the world's biggest sponsor of malicious cyber operations[316] – has the principle of sovereignty as the cornerstone of its national and international cyber policy, where it has stated that no "infringement of sovereignty in cyberspace will be tolerated, the rights of all countries to independently choose their development path, network management method and Internet public policy, as well as to equally participate in international cyberspace governance will be respected."[317]

On the other hand, the Russian Information Security Strategy[318] differentiates between cyber sovereignty and technological sovereignty.[319] Moreover, in February 2019, the so called "digital sovereignty bill" or "sovereign internet" law was approved by the Russian Parliament.[320] The bill was described as nationalizing the country's Internet (known as Runet) and thus isolating it from the global Internet network.[321] Furthermore, the Runet would be able to close international connections as well as monitor, filter and restrict incoming Internet traffic.[322] This "Internet Iron Curtain" became reality when the bill

[313] Väljataga (n 93), p. 7. See also Justin Sherman, 'How Much Cyber Sovereignty is Too Much Cyber Sovereignty?', 30 October 2017, Council on Foreign Relations, https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

[314] Press statements following Russian-Chinese talks, 25 June 2016, http://en.kremlin.ru/events/president/transcripts/52273.

[315] Joint Statement Between The Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

[316] Väljataga (n 93), p. 7.

[317] 'International Strategy of Cooperation on Cyberspace Contents' (2017), unofficial English translation available at http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm. See also Hao Yeli, 'A Three-Perspective Theory of Cyber Sovereignty' (2017). Moreover, for an interesting read on the Chinese views on sovereignty in cyberspace, see Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realization', in Governing Cyberspace: Behavior, Power, and Diplomacy (2020), pp. 107-132; Väljataga (n 93), p. 7.

[318] Russian Federation, 'Doctrine of Information Security of the Russian Federation', 5 December 2017, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

[319] Väljataga (n 93), p. 7.

[320] Adrian Venables, 'Establishing Cyber Sovereignty – Russia Follows China's Example', 20 March 2019, https://icds.ee/establishing-cyber-sovereignty-russia-follows-chinas-example/.

[321] Ibid.

[322] Ibid.

came into force in November 2019.[323] In other words, Russia seeks to route its Internet traffic and data through state controlled points.[324] Whilst the Kremlin has stated that the law will significantly improve the cyber security and increasingly protect the country from foreign cyber operations, critics fear that "Russia's campaign to control its cyber borders mirrors the 'great firewall of China' that restricts the viewing habits of the largest population of Internet users in the world."[325] Furthermore, Russian state intelligence organizations have on several occasions been accused of conducting malicious cyber operations and the attribution of these activities is partially due to the ability to trace the operation back to its source, and the "requirement to pass through state-controlled entry points may inhibit this activity and reduce the effectiveness of tracing the origin of malicious cyber activity."[326]

In essence, it has become apparent, that two differing views (among Western states at least) on how international law applies to state cyber operations have emerged.[327] The different views can be divided into two camps – on one hand, the proponents of a "sovereignty as a principle" and on the other there are advocates of a "sovereignty as a primary rule." The "sovereignty as a rule approach" has also been further divided into two different approaches – a *de minimis* approach, according to which a *de minimis* threshold must be crossed in order to find a violation of sovereignty, and a penetration-based approach which maintains that every penetration of a state's computer network located within the territory of a state will violate that state's sovereignty.[328]

3.4 Cyber operations as a violation of state sovereignty

A central ongoing debate in the cyber context is whether sovereignty is a general principle of international law or is there a cyber specific rule of sovereignty. Critics claim that sovereignty is merely "a background rule rather than a primary rule – and that it binds

[323] BBC News, 'Russia internet: Law introducing new controls comes into force', 1 November 2019, https://www.bbc.com/news/world-europe-50259597.
[324] Ibid.
[325] Adrian Venables, 'Establishing Cyber Sovereignty – Russia Follows China's Example', 20 March 2019, https://icds.ee/establishing-cyber-sovereignty-russia-follows-chinas-example/.
[326] Ibid.
[327] Moynihan (n 4), p. 8.
[328] Przemyslaw Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (2020), p. 4.

states only inasmuch as it informs other rules of international law, most prominently those prohibiting the threat or use of force or intervention in the internal affairs of other states."[329] However, for instance, the prohibition on the use of force contains thresholds that are seldom reached with respect to cyber activities, and thus "the vast majority of hostile cyber operations attributable to states implicate only the prohibition of violation of sovereignty."[330]

Accordingly, one of the most central legal issue with respect to cyberspace is *when* cyber operations directed at a state violate its sovereignty. Rule 4 of the Tallinn Manual states that a "State must not conduct cyber operations that violate the sovereignty of another State."[331] The Manual further provides, that "cyber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of sovereignty and are prohibited by international law."[332] A more complicated issue is whether there exists a threshold for violations of sovereignty. If a state agent is physically present on the territory of another state without permission, does the mere presence violate territorial sovereignty, or does the state agent need to conduct harmful activities on the territory of that state in order for the threshold to be reached?[333]

Subsequently, the precise threshold for a violation of sovereignty is unsettled. The International Group of Experts (IGE) agreed that whenever a state physically crosses into the territory or national airspace of another state without consent, a violation of sovereignty would take place.[334] Similarly, in the cyber context, it is a violation of sovereignty "for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there."[335] For instance, in 2018, the Russian military intelligence agency (GRU), attempted to conduct a cyber operation

[329] Phil Spector, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017), p. 219.
[330] Schmitt, Vihul (n 312), p. 214.
[331] Tallinn Manual 2.0, Rule 4 – Violation of Sovereignty, p. 17.
[332] Tallinn Manual 2.0, p. 17.
[333] Harriet Moynihan, 'The Application of International Law to Cyberspace: Sovereignty and Non-intervention', 13 December 2019, Just Security, https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.
[334] Tallinn Manual 2.0, p. 19.
[335] Tallinn Manual 2.0, p. 19. The Manual gives the following example: "If an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place". Ibid.

against the Organization for the Prevention of Chemical Weapons (OPCW), located in The Hague, while physically present on Dutch territory.[336]

That said, cyber operations conducted remotely from outside the territory of the target state are more commonplace.[337] However, the legal character of these so-called remote cyber operations is unresolved in international law.[338] The lawfulness of cyber operations was assessed on two different bases: 1) "the degree of infringement upon the target State's territorial integrity"[339]; and 2) "whether there has been an interference with or usurpation of inherently governmental functions."[340] In other words, a cyber operation will violate sovereignty only if they cause a certain level of harm on the territory of the victim state.

Regarding the first base, the Tallinn Manual 2.0 sets out a hierarchy of scenarios whereby cyber operations constitute a violation of sovereignty; in other words, cyber operations violate sovereignty if they cause: "(1) physical damage[341]; (2) loss of functionality[342]; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality[343]."[344] Accordingly, the majority of the Experts agreed that whenever cyber operations result in physical damage or injury it would qualify as a violation of sovereignty, as in the case of non-consensual physical presence on the victim state's territory to conduct cyber operations.[345] On the other hand, the experts could not agree

[336] Government of the Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', 4 October 2018, available at https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw. Several states have condemned the Russian cyber operation against OPCW and commended the Dutch efforts to bring the attack to a halt, see e.g. https://www.un.org/press/en/2018/gadis3601.doc.htm. See also 'Joint Statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian Cyber Attacks' 4 October 2018, https://www.consilium.europa.eu/sv/press/press-releases/2018/10/04/joint-statement-by-presidents-tusk-and-juncker-and-high-representative-mogherini/.
[337] Moynihan (n 4), p. 19.
[338] Tallinn Manual 2.0, p. 20.
[339] Ibid.
[340] Ibid. Inherently governmental functions include e.g. the holding of elections or the collection of taxes. Accordingly, a DDoS attack which effects to collection of taxes would thus be a violation of sovereignty.
[341] Tallinn Manual 2.0 gives the example of "malware that causes the malfunctioning of the cooling elements of equipment, thereby leading to overheating that results in the components melting down." Tallinn Manual 2.0, p. 20; Moynihan (n 4), p. 21.
[342] For example, "hacking into a computer and spreading a powerful virus that disables functionality, potentially also resulting in the need to replace computers…" Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention' (2019), p. 21.
[343] Tallinn Manual 2.0, p. 21: "a cyber operation causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences…"; Moynihan (n 4), p. 21.
[344] Tallinn Manual 2.0, p. 20.
[345] Ibid.

upon the precise meaning of "loss of functionality", as for some it denoted an irreparable loss of function, and for others it designated situations where physical repair was necessary (e.g. to replace computer hardware).[346]

Conversely, no consensus could be reached as to whether cyber operations that result neither in physical damage nor loss of functionality could amount to a violation of sovereignty.[347] For instance, the deletion of a state's confidential critical data by another state is not likely to result in physical damage or loss of functionality, "but may have a more serious effect on the ability of the target [state] to exercise its sovereign functions."[348] The idea of a violation measuring harm seems to have been partially inspired the "effects doctrine" from the context of the rules on the use of force, which the Experts also considered in the context of state cyber attacks.[349]

Moreover, the second basis upon which the Experts determined a violation of sovereignty was when one state's cyber operations "interfere with or usurps the inherently governmental functions of another State,"[350] since states have the exclusive right to perform set functions. However, no exact definition of the notion of "inherently governmental functions" was agreed upon, but several examples were given, such as altering or changing data in a way that it interferes with a state's ability to deliver social services, hold elections, collect taxes, engage in diplomatic relations or hinders the performance of key national defense agencies.[351] Beyond these "self-evident examples", the notion of inherently governmental functions became less clear.[352] While the Tallinn Manual 2.0 specifies that the beforementioned basis need not result in physical damage, injury or loss, it is not specified whether a cyber operation that causes physical or

[346] Michael Schmitt, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018), p. 44. Schmitt states that he is in favor of the latter position since "the essence of sovereignty is control by the State over activities on its territory; remote cyber operations that necessitate reloading or replacement represent a significant intrusion on that legal prerogative."
[347] Tallinn Manual 2.0, p. 21.
[348] Harriet Moynihan, 'The Application of International Law to Cyberspace: Sovereignty and Non-intervention', 13 December 2019, Just Security, https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.
[349] Moynihan (n 4), p. 22. The Tallinn Manual 2.0 (and in the first edition) puts forth the so-called 'Schmitt-criteria' according to which a cyberattack constitutes a use of force. The seven criteria are: severity; immediacy; directness; invasiveness; measurability of effects; military character; state involvement; and presumptive legality. See Tallinn Manual 2.0, pp. 334-336; Tallinn Manual 1.0, pp. 49-52.
[350] Tallinn Manual 2.0, p. 21.
[351] Tallinn Manual 2.0, p. 22.
[352] Michael Schmitt, 'In Defense of Sovereignty in Cyberspace', 8 May 2018, Just Security, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

functional damage needs to also interfere or usurp the inherently governmental functions of the victim state.

What can be concluded from the Tallinn Manual 2.0 position is that an effects-based approach is applied, where the unlawfulness of a malicious cyber operation is determined based on the physical damage or injury it results in, and thus the Experts agreed that "sovereignty is both a principle of international law from which certain rules, such as the prohibition of intervention into the external or internal affairs of other states, derive, *and* a primary rule of international law susceptible to violation."[353]

In the case of WannaCry, did the ransomware attack violate the sovereignty of the affected states? As established, a violation of sovereignty occurs whenever a cyber operation either causes damage to, or loss of function of cyber infrastructure in another state or it interferes with inherently governmental functions. WannaCry consisted mainly of data blockage and intrusion into numerous computer systems around the world.[354] However, WannaCry mostly falls into the gray zone in which the threshold of violation remains undetermined.[355] While some have maintained that WannaCry did amount to a violation of territorial sovereignty,[356] it has been held that "this approach overemphasizes physical effects on territory, while omitting a crucial aspect of sovereignty, namely the exercise of state power."[357]

Albeit no cyber infrastructure being physically damaged, WannaCry did, for instance, affect thousands of computers belonging to the Russian Ministry of Interior, which could be seen as interfering with "inherently governmental functions."[358] Cyber operations that interfere with inherently governmental functions are a violation of sovereignty and therefore an internationally wrongful act.[359]

---

[353] Ibid; Moynihan (n 4), p. 22; Tallinn Manual 2.0, p. 333.
[354] Delerue (n 48), p. 231.
[355] Michael Schmitt, Sean Fahey, 'WannaCry and the International Law of Cyberspace', 22 December 2017, Just Security, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/;
[356] Delerue (n 48), p. 231.
[357] Przemyslaw Roguski, 'Violations of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach', p. 74, in Dennis Broeders, Bibi van deb Berg (ed), 'Governing Cyberspace: Behavior, Power, and Diplomacy (2020).
[358] CCDCOE, 'WannaCry Campaign: Potential State Involvement Could Have Serious Consequences' (2017), https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/. Radoslaw Fordonski, Wojciech Kasprzak, 'WannaCry ransomware cyberattack as a violation of international law' (2019), p. 53.
[359] Tallinn Manual 2.0, p. 21.

3.5 Sovereignty – primary rule or principle?

It is vital to emphasize the importance of states to publicly articulate their views of international law, especially in cyberspace. However, only a handful of states have publicly put forth their views on violations of sovereignty in cyberspace, but states are nonetheless beginning to be more vocal about their positions. The "sovereignty as a primary rule" adopted by the Tallinn Manual 2.0 was reportedly not challenged by any of the fifty states that gave unofficial feedback during the manual's drafting process.[360] In September 2019, France published a document setting out the French position on how international law applies in cyberspace, clearly stating that cyber operations may constitute a violation of sovereignty.[361] The document further provides that:

> Any cyberattack against French digital system or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.[362]

In other words, France confirms that should it be the victim of such an attack, it can respond diplomatically, through countermeasures or even employ its armed forces if the cyber operation amounts to an armed attack.[363] Furthermore, the 20-page document was a powerful statement of "France's intent to shape the future discussions on the applicability of international law in cyberspace."[364]

Similarly, in July 2019, the Dutch Minister of Foreign affairs also opined on the applicability of sovereignty in cyberspace:

> According to some countries and legal scholars, the sovereignty principle does not constitute an independently binding rule of international law that is separate from the other rules derived from it. The Netherlands does not share this view. It believes that respect for the sovereignty

[360] See chapter 1.3. See also, Michael N. Schmitt, Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017), p. 1649: "… a draft of the *Tallinn Manual 2.0* rule on violation of sovereignty and its accompanying commentary was discussed in three meetings of over fifty States and … they voiced no meaningful objection to Rule 4."
[361] Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberspace', 9 September 2019.
[362] France, International Law Applied to Operations in Cyberspace (official English translation), p. 6.
[363] Ibid.
[364] Przemyslaw Roguski, 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I', 24 September 2019, Opinio Juris, http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.

> of other countries is an obligation in its own right, the violation of which may in turn constitute and internationally wrongful act.[365]

As was already mentioned earlier, the Netherlands is not a stranger to cyber operations, taking into consideration the attempted Russian military intelligence (GRU) hacking of the OPCW, and therefore, the letter is a major contribution to the ever growing, and much needed, body of *opinio juris* on the subject of international law and cyberspace.[366] Moreover, as the Tallinn Manual 2.0 concluded, both France and the Netherlands pointed out, that the challenge still lies in determining exactly which remote cyber operations constitute a violation of sovereignty. The Estonian President also confirmed that sovereignty "entails not only rights, but also obligations."[367] Recently, in February 2020, the Czech Republic stated that it "concurs with those considering the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation."[368]

In sharp contrast, the opposing view is that sovereignty is a principle that may guide state interactions in cyberspace but does not in itself constitute a standalone primary rule. Accordingly, some states have been reluctant to confirm the principle of sovereignty as one that prohibits certain types of cyber operations.[369] The reluctance is tangible, especially within the UN GGE, the main state level forum in which international law where a significant amount of cyber related debates take place.[370] To date, only one state has publicly rejected the existence of an international law rule safeguarding sovereignty

---

[365] The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, p. 2.
[366] Michael Schmitt, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis', 14 October 2019, Just Security, https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.
[367] Kersti Kaljulaid, President of the Republic at the Opening of CyCon 2019, https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/. See also Michael Schmitt, 'Estonia Speaks Out on Key Rules for Cyberspace', 10 June 2019, Just Security https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.
[368] Czech Republic, Statement by Mr. Richard Kadlcak, Special Envoy for Cyberspace, 2nd substantive session on the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, 11 February 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.
[369] Schmitt, Vihul (n 312), p. 214.
[370] Ibid. See e.g. UN GGE 2013 Report, paras. 20, 27.

– the United Kingdom.[371] The United Kingdom has opined that a cyber specific rule of sovereignty does not exist in cyberspace, stating that sovereignty is a generally recognized rule of international law from which other principles and prohibitions derive from. Accordingly, in May 2018, the former Attorney General Jeremey Wright set forth the British position on the international law applicable to cyberspace:

> Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.[372]

The statement seems to be a clear rejection of the Tallinn Manual 2.0 position, which stated that sovereignty is an independent legal rule prohibiting certain cyber operations. According to this view, cyber operations can never violate the sovereignty of a state but may amount to other internationally wrongful acts on the basis of, e.g. prohibited intervention or the use of force. Put differently, according to the United Kingdom, the principle of sovereignty does not create autonomous and separate legal obligations but is protected under other established rules of international law.

Interestingly enough, if the United Kingdom believes that sovereignty is not a rule that can be violated by a cyber operation, why did UK's National Cyber Security Center (NCSC), together with the United States[373] and the European Union,[374] publicly attribute a series of cyber operations against Georgia to the Russian military intelligence

[371] Jeffrey Biller, Michael Schmitt, 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences' 24 October 2018, EJIL:Talk! https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/.
[372] Jeremy Wright, 'Cyber and International Law in the 21st Century', 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[373] The US Department of State, Statement by the Secretary of State Michael R. Pompeo, 'The United States Condemns Russian Cyber Attack Against the Country of Georgia', 20 February 2020, https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.
[374] Council of the European Union, 'Declaration by the High Representative on behalf of the European Union – call to promote and conduct responsible behaviour in cyberspace', 21 February 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/.

service?[375] Despite the lack of evidence presented by the states,[376] the NCSC specifically stated "with the highest level of probability that on 28 October 2019 the GRU carried out cyber attacks in … an attempt to undermine *Georgia's sovereignty*, to sow discord and disrupt the lives of ordinary Georgian people."[377] The substantially coordinated cyber operations rendered thousands of websites inoperable, including the presidential website as well as the national TV station.[378] Although the cyber operation itself was technically unsophisticated, the scale of the incident was unprecedented.[379] However, if sovereignty is merely a principle of international law, exactly which rule of international law did Russia violate? The cyber attack did not amount to a use of force, nor did it constitute a prohibited intervention since targeting the functionality of governmental websites or servers does not amount to coercion on a state's free exercise of its sovereign will.[380]

For the time being, the United Kingdom is relatively alone in disputing of the violability of sovereignty in cyberspace. However, in 2017, a Memorandum issued by the outgoing General Counsel of the U.S. Department of Defense (DoD) seemed to question the "sovereignty as a rule" principle, and thus taking a somewhat similar position as the United Kingdom on sovereignty.[381] The Memorandum observes that "[m]ilitary cyber activities that are neither a use of force, nor violate the principle of non-intervention are largely unregulated by international law at this time"[382] Conversely, the statement seems to be contradictory to other previous statements issued by U.S. government officials, which they have "foreseen a role for sovereignty in the application of international law to

---

[375] United Kingdom, 'UK condemns Russia's GRU over Georgia cyber-attacks', 20 February 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

[376] Przemyslaw Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, Just Security, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

[377] United Kingdom, 'UK condemns Russia's GRU over Georgia cyber-attacks', 20 February 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks. Emphasis added by author.

[378] BBC News, 'Georgia hit my massive cyber-attack', 28 October 2019, https://www.bbc.com/news/technology-50207192.

[379] Przemyslaw Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, Just Security, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

[380] Ibid.

[381] Moynihan (n 4), p. 9.

[382] Quote taken from Sean Watts, Theodore Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018), p. 828. After having circulated internationally, the memo was classified and therefore designated "For Internal Use", see Michael Schmitt, 'In Defense of Sovereignty in Cyberspace', 8 May 2018, Just Security, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

cyberspace."[383] For instance, in 2012, the former Legal Advisor for the U.S. Department of State, Harold Koh, stated that "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict."[384]

Since the 2017 Memorandum was deemed classified, Robert Taylor and Gary Corn[385] have shun some light on the matter, maintaining the view that sovereignty does not operate as a rule of international law:

> However, law and state practice instead indicate that sovereignty serves as a principle of international law that guides state interactions but is not itself a binding rule that dictates results under international law. While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects to not rise to the level of an unlawful use of force of an unlawful intervention.[386]

The view put forth by the United States, however, seems to be somewhat conflicting. It proclaims that sovereignty should "guide state interaction" and "factor into the conduct of every cyber operation", while simultaneously disputing that sovereignty prohibits state cyber operations. Corn and Taylor further claimed that there is insufficient state practice or *opinio juris* supporting the claim that the principle of sovereignty may function as a standalone, binding rule of customary international law.[387] This was further echoed in 2020, as the U.S. Cyber Department of Defense (DoD) General Counsel Paul Ney gave a speech, in which he stated that "[f]or cyber operations that would not constitute a prohibited intervention or use-of-force … there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that

---

[383] Moynihan (n 4), p. 9.
[384] Harold Hongju Koh, 'International Law in Cyberspace', 18 September 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. Furthermore, already in 1999, the US Department of Defense stated that "An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty." See US Department of Defense, Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations', May 1999, available at https://fas.org/irp/eprint/io-legal.pdf.
[385] Michael N. Schmitt, Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017), pp. 1641-1642: "Considering their positions as, respectively, the most senior legal advisor for the U.S. organization that engages in military cyber operations, the author of the memorandum, and a highly placed DoD attorney at the time it was issued, it is reasonable to assume that their views are consistent with the DoD's position."
[386] Corn, Taylor (n 310), p. 208.
[387] Ibid.

customary international law generally prohibits such non-consensual cyber operations in another State's territory."[388]

In the speech, it was also argued that the state silence "in the face of countless publicly known cyber intrusions" would preclude the existence of an international prohibition against such operations.[389] Keeping in mind that state silence can contribute to the formation of customary international law, remaining silent on a certain matter does not automatically imply that a state acknowledges or rejects the existence of a specific rule of international law.[390] States need to be in a position to react, as well as the circumstances must call for such a reaction.[391] Put differently, states must have knowledge of the practice in order to react. For instance, due to publicity given to a certain practice it can be assumed that the state was aware of it and thus having ample time and capability to act.[392] Therefore, when these prerequisites are not met, state inaction cannot "be attributed to an acknowledgment that such practice was mandated (or permitted) under customary international law."[393] Moreover, the U.S. position seems to denote that the existence of an obligation to respect sovereignty is cyberspace must be established by widespread and coherent state practice and *opinio juris*, instead of stemming from the general applicability of extant international law to cyber activities.[394] As the ICJ has affirmed, an international legal instrument "has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation."[395]

---

[388] U.S. Department of Defence, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference', 2 March 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

[389] Ibid.

[390] Przemyslaw Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', Just Security, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

[391] ILC Draft Conclusion, para. 10 (3), p. 140 https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.

[392] Ibid, p. 142.

[393] Ibid.

[394] Przemyslaw Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', Just Security, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

[395] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, ICJ Reports 1971, p. 19. See also Vienna Convention on the Law of Treaties, art. 31 (3) (b).

Also, suggesting that numerous states have remained silent does not correlate with current state practice. Since July 2019, five states have come out in favor of the "sovereignty-as-a-rule" approach,[396] most recently Finland.[397] In addition, that a considerable amount of state cyber operations are conducted in secrecy, and that states might not want to disclose highly sensitive information relating to their cyber defence capabilities, the recent Austrian position explicitly refers to being the victim of a severe cyber operation.[398] In other words, states affected by malicious cyber operations do issue their views on the matter when deemed appropriate.

3.6 Cyber operations as a violation of the principle of non-intervention

The legal obligation not to intervene in another states internal or external affairs is "the corollary of every State's right to sovereignty, territorial integrity and political independence."[399] The principle of non-intervention in the internal or foreign affairs of another state derives from the notion of sovereign equality of states.[400] Despite not being explicitly regulated in the UN Charter, the principle stems primarily from the notions of sovereignty and territory,[401] and it has been confirmed as a rule of international custom.[402]

---

[396] Przemyslaw Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', Just Security, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

[397] Finnish Ministry for Foreign Affairs, p. 3, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727:"Finland sees sovereignty as a primary rule of international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility."

[398] Open-ended working group on developments in the field of information and telecommunications in the context of international security – Second substantive session (10-14 February 2020), http://webtv.un.org/search/3rd-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131646836001/?term=Second%20substantive&lan=english&sort=date&page=2 ; Pre-Draft Report of the OEWG – ICT, Comments by Austria, 31 March 2020, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf; Przemyslaw Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', Just Security, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

[399] Oppenheim's International Law, 9th ed. 1992, p. 428, quoted in Michael Schmitt, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018), p. 48.

[400] Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' (2013), p. 164.

[401] Nicaragua, para. 251: "The effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and non-intervention."

[402] ICJ, Corfu Channel para. 35; Nicaragua, para. 202; See also e.g. Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the

Subsequently, as an accepted customary norm, the principle of non-intervention applies to state activities in cyberspace.[403] The Tallinn Manual 2.0 provides that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[404] Accordingly, an illegal intervention takes place when a state interferes with the affairs of another state's *domaine reservé,*[405] namely matters which each state has the right to decide upon freely,[406] in order to coerce it into certain behavior.[407] In the cyber context, an example of the latter would be the launching of a cyber operation in order to manipulate another state's election by remotely altering electronic ballots, thus affecting the voting system and possibly the entire outcome of the election.[408] Whereas the 2016 DNC hack against the United States might be the most infamous example of election intervention, other states such as France,[409] Germany,[410] and the Netherlands[411] have also allegedly been victims of such intervention.[412] Accordingly, cyber operations are seemingly thought of as a good method for coercing a state.[413]

As affirmed by the ICJ, the requirement of coercion constitutes a fundamental element of the non-intervention rule[414] and the Tallinn Manual 2.0 defines coercion as "an

---

Charter of the United Nations, Principle 3 (UN Doc. A/RES/25/2625, Oct. 2, 1970): "No State may … coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind."

[403] UN GGE Report 2015, UN Doc. A/70/174, para. 28(b).

[404] Tallinn Manual 2.0, Rule 66 – Intervention by States, p. 312. The IGE also reaffirmed the customary nature of the rule of non-intervention.

[405] "The notion of domaine reserve (reserved domain) describes the areas of State activity that are internal or domestic affairs of a State and are therefore within its domestic jurisdiction or competence […] Its precise content may vary over time according to the development of international law, but the closely linked principle of sovereignty of States entails that at least some matters remain within the regulatory competence of States." Katja S Siegler, 'Domaine Reservé' MEPIL, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398.

[406] Nicaragua, para. 205.

[407] Nicaragua, para. 202; Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' (2013), p. 164.

[408] Tallinn Manual 2.0, p. 312; Efrony, Shany (n 102), p. 642.

[409] Emmanuelle Walkowiak, 'Russia's meddling in the French elections: How and why?', 24 May 2017, available at https://electionwatch.unimelb.edu.au/articles/russias-meddling-in-the-french-elections-how-and-why.

[410] Sumi Somaskanda, 'The Cyber Threat To Germany's Elections Is Very Real', 20 September 2017, available at https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162/.

[411] Nick Allen, 'Dutch spies 'caught Russian election hackers on camera', 26 January 2018, https://www.telegraph.co.uk/news/2018/01/26/dutch-spies-caught-russian-election-hackers-camera/.

[412] Efrony, Shany (n 102), p. 642.

[413] Delerue (n 48), p. 239.

[414] Nicaragua, para. 205: "[t]he element of coercion … defines, and indeed forms the very essence of prohibited intervention …."

affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[415] However, the notion of "coercion" is unsettled and the difficulties regarding the precise scope and definition of the element of coercion have been acknowledged by various states.[416] Accordingly, it is unclear whether or not states apply the same threshold of coercion, seeing as "some States – in particular those which deny the existence of a rule of territorial sovereignty in cyberspace – might apply a broader standard to compensate for the lack of a prohibition of low-intensity cyber operations."[417]

Some states have given examples of cyber operations which may amount to illegal intervention. For instance, in addition to the example of election meddling, interference which causes harm to a state's political, economic, social or cultural system may be in violation of the principle of non-intervention.[418] Further examples given by Australia include interference in the fundamental operations of parliament or intervention in the stability of a state's financial system.[419] It has even been suggested that foreign influence operations using covert activities, for instance the spreading of fake news or usage of social media to impact voter behavior may amount to illegal coercive intervention.[420]

Did WannaCry constitute a coercive interference into the *domain reservé* of the affected states? Put shortly, despite being destructive, there was a clear lack of intention to coerce and thus failing to amount to an unlawful intervention in the internal or external affairs of the states involved. That said, could WannaCry have amounted to an "usurpation of an inherently governmental function?"[421] Whereas the primary target of the ransomware attack was private organizations for financial gain, many governmental computer systems across the world were hit. For instance, Brazil's Foreign Ministry was affected as well as

[415] Tallinn Manual 2.0, p. 317.
[416] Roguski (n 328), p. 8.
[417] Ibid.
[418] France, 'International Law Applied To Operations in Cyberspace' p. 7.
[419] Australia, 'Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace' (2019), available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.
[420] Efrony, Shany (n 102) p. 642; See also Harold Hongju Koh, 'The Trump Administration and International Law' (2017), p. 450: "Although the international law of cyberspace is in its infancy, even if the Russians did not actually manipulate polling results, illegal coercive interference in another country's electoral politics – including the deliberate spreading of false news – constitutes a blatant intervention in violation of international law."
[421] Tallinn Manual 2.0, p. 24. Fordonski, Kasprzak (n 358), p. 61.

various court system computers across the country were infected.[422] However, WannaCry did not explicitly target the state apparatus or affect any vital computer systems but rather the "infected computers [were] part of antiquated systems not deemed important enough to update with the latest security patches, rather than machines integral to the company's core business."[423] In sum, the WannaCry ransomware attack did not fulfill the two conditions precedent to finding a violations of the prohibition on non-intervention.

On the other hand, at the time of writing, the recent cyber operations related to the coronavirus pandemic, provided that they are attributed to a state, would amount to unlawful intervention.[424] For instance, the disabling cyber operations against the coronavirus testing facility in the Czech Republic could be seen as hindering the state to fully carry out its national crisis management plan for managing the ongoing pandemic.[425]

When a cyber operation is conducted, or any other internationally wrongful act, international law sets out the parameters within which the injured state can respond. The law on state responsibility permits injured states to take measures that would under normal circumstances amount to breaches of international law in order to address a prior breach by another state. It is thus crucial to identify the perpetrating state, since the absence of attribution precludes state responsibility.[426] Accordingly, the remaining chapters of the thesis will delve into the cyber attribution process and the underlying difficulties therein, as well as analyse the possible response options available for injured states.

---

[422] Data Protection, 'WannaCry Ransomware Attack Summary', 17 May 2017, https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/; Fordonski, Kasprzak (n 358), p. 61.
[423] Jack Stubbs, 'Exclusive: Wannacry hits Russian postal service, exposes wider security shortcomings', 24 May 2017, Reuters, https://www.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUSKBN18K26O; Fordonski, Kasprzak (n 358), p. 61.
[424] Schmitt (n 94), p. 40.
[425] Ibid. For further reading upon malicious cyber operations conducted during the Covid-19 pandemic, see Marko Milanovic, Michael N. Schmitt, 'Cyber Attacks and Cyber (Mis)information during a Pandemic' (2020).
[426] Banks (n 50), p. 1495.

4. Attribution of cyber operations

4.1 Current state of affairs

"Attribution is the art of answering a question as old as crime and punishment: who did it?"[427] Attribution refers to the process of attributing a certain act or conduct to the perpetrator, and the question of how to attribute state responsibility in the cyber context has been recognized as a considerable hurdle.[428] However, the identification of the machines behind the launching of cyber operations is no longer the crux of the issue for technologically advanced states, but rather the identification of the persons, organizations or states that are legally responsible for the cyber conduct.[429]

Attribution is essential, as it constitutes one of the constitutive elements of state responsibility and forms the legal basis for the potential responses taken by the victim state. On that account, states view cyber attribution as something important precisely because the absence of attribution precludes state responsibility.[430]An assessment of attribution is not merely a statement of who conducted the cyber operation, but rather a sequence of events and judgements illustrating whether it was an isolated incident, and identifying the possible perpetrator and incentives, as well as assessing whether a foreign government had a prominent role in ordering or leading the operation. [431] In the last few years, the international community has witnessed a significant increase in states willing to publicly attribute cyber operations to other states, something that they were previously rather reluctant to do.[432] Moreover, states have begun cooperating and working together to collectively attribute state cyber operations.[433] In other words, the attribution is

[427] Thomas Rid, Ben Buchanan, 'Attributing Cyber Attacks' (2015), p. 4.
[428] See e.g. Scott J. Shackelford, 'State Responsibility For Cyber Attacks: Competing Standards For A Growing Problem' (2010).
[429] Banks (n 43), p. 192.
[430] Banks (n 50), p. 1495.
[431] Office of the Director of National Intelligence, 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', 6 January 2017, p. 2, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[432] Moynihan (n 4), p. 4.
[433] CCDCOE, 'Trends in international law for cyberspace', p. 2, 24 May 2019, https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf. For instance, in the case of GRU's cyber

increasingly of a collective nature, where several states issue joint attribution claims, as was the case with for example the cyber operations against OPCW[434] and Georgia.[435] Steps have also been taken towards creating a structure for collective attribution, where a noteworthy example is the EU Cyber Diplomacy Toolbox from 2017,[436] and the 2019 EU sanctions regime.[437]

Since 2007, there have been more than twenty "high profile attribution claims" of state affiliated cyber operations.[438] The latter shows that malicious cyber activity in cyberspace is perceived as a real problem requiring coordinated and unified state responses.[439] Furthermore, as malicious cyber activity has become commonplace, states have also begun investing in greater efforts of accurate attribution, since when no attribution is done or it is done inaccurately, states lose credibility and effectiveness in dealing with malicious activities that harm the state as well as its citizens.[440] The United States and the United Kingdom, for instance, have invested significantly in attribution technologies and attribution is regarded as a fundamental component in the effectiveness of cyber

operation against Georgia in late 2019, several states attributed the cyber incident to Russia. Among these states were the U.S., the U.K., Australia, Ukraine, and the European Union. Giorgi Nakashidze, 'Cyberattack against Georgia and International Response: emerging normative paradigm of 'responsible state behavior in cyberspace'?, 28 February 2020, https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/.

[434] Government of the Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', 4 October 2018, available at https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw; Joint statement by Prime Minister May and Prime Minister Rutte on cyber activities of the Russian military intelligence service, the GRU, 4 October 2018,https://www.government.nl/latest/news/2018/10/04/joint-statement-by-prime-minister-may-and-prime-minister-rutte-on-cyber-activities-of-the-russian-military-intelligence-service-the-gru

[435] Przemyslaw Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/; Yuval Shany, Michael N. Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) p. 211.

[436] Erica Moret, Patryk Pawlak, 'The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?' (2017), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf ; https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/ ; "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, June 7, 2017); Moynihan (n 4), p. 54.

[437] Council Decision (CFSP) 2019/797 of 17 May 2019, Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or its Member States, 2019 O.J. (L 129) 13 (EC);

[438] Nicholas Tsagourias, Michael D. Farrell, 'Cyber attribution: technical and legal approaches and challenges' (2020), p. 1.

[439] Przemyslaw Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

[440] Banks (n 43), p. 192; ICDS, 'Attribution of Major Cyber-attacks Has Become Mainstream', 16 January 2019, https://icds.ee/en/attribution-of-major-cyber-attacks-has-become-mainstream/.

deterrence.[441] Moreover, the United States has even published a Guide to Cyber Attribution.[442]

Attribution of cyber operations has technical, legal and political aspects.[443] The technical aspects of attribution refer to the technical forensics used to determine the origin of a cyber activity.[444] Most importantly, the attribution process under international law should be distinguished from public attribution, which is the political decision of a state to name the responsible entity behind a cyber operation, usually without attaching legal consequences.[445] Correspondingly, several cyber operations have been publicly attributed to a state, for instance WannaCry to North Korea,[446] and NotPetya to the Russian Federation.[447] However, the cyber operations were not characterized under international law, thus further illustrating the difficulties of applying international law to abstruse cyber scenarios.[448] In effect, public attribution claims have thus far consisted of unilateral accusations by the victim state, often echoed by its allies, followed by subsequent denial by the accused state.[449] To illustrate, Russia firmly denied the collective attribution claims

[441] "On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace." The US Department of Defense, 'The Department of Defense Cyber Strategy' (2015), pp. 11-12, https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf. See also United Kingdom, 'National Cyber Security Strategy 2016-2021, HM Government, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf; Nicholas Tsagourias, Michael D. Farrell, 'Cyber attribution: technical and legal approaches and challenges' (2020).

[442] Office of the Director of National Intelligence, 'A Guide to Cyber Attribution', 14 September 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

[443] Tsagourias (n 57), p. 233.

[444] Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' Hoover Working Group on National Security, Technology and Law', p. 6. For an interesting read on technical methods of attribution, see Andrew Nicholson et al, 'A Taxonomy of Technical Attribution Techniques for Cyber Attacks' (2012).

[445] François Delerue, 'International Law in Cyberspace Matters: This is How and Why' (2019), p. 1.

[446] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, December 19, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/; https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ "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."

[447] BBC News, 'UK and US blame Russia for 'malicious' NotPetya cyber-attack', 15 February 2018, https://www.bbc.com/news/uk-politics-43062113; CRF, https://www.cfr.org/cyber-operations/notpetya.

[448] Michael Schmitt, Jeffrey Biller, 'The NotPetya Cyber Operation as a Case Study of International Law', July 11 2017, EJIL: Talk! https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/

[449] Sharngan Aravindakshan, 'Cyberattacks: a look at evidentiary thresholds in International Law' (2020), p. 4.

over the alleged Russian authorship of the cyber operation against OPCW, calling the joint attribution "Western spy mania" and "yet another state-managed propaganda campaign."[450]

It must be noted, that while public attribution of cyber operations are progressively being used by governments to establish a framework of acceptable state behavior in cyberspace, a significant trend in the field of attribution has been the increasing involvement of private sector cybersecurity companies in attributing cyber operations to both states and non-state actors.[451] Between 2016 and 2018, 85 % of the cyber operations conducted resulted in a public attribution of some form, of which only 15 % were issued by states' governments.[452]

Public attribution of cyber operations constitutes one of the primary sources from which the public learns about who is attacking whom in cyberspace, hence influencing the threat landscape and perception of the general public.[453] When looking at past cyber incidents, however, it becomes evidently clear that the same few state actors have been more involved in public attribution claims than others. Specifically, the Netherlands and the so called Five Eyes[454] – the United States, the United Kingdom, Canada, Australia and New Zealand – have been the most active nations in condemning malicious state activity in cyberspace.[455] Several reasons behind why only a limited number of states are engaging

[450] BBC News, 'Russia cyber-plots: US, UK and Netherlands allege hacking', 4 October 2018, https://www.bbc.com/news/world-europe-45746837.
[451] Anushka Kaushik, 'Public attribution and its scope and efficacy as a policy tool in cyberspace' (2019), https://www.orfonline.org/expert-speak/public-attribution-and-its-scope-and-efficacy-as-a-policy-tool-in-cyberspace-56826/. A notable example is the cybersecurity company CrowdStrike, who within a day after the DNC realized they had been hacked, managed to identify two Russian state-sponsored hacking groups behind the hack and published a detailed analysis of its findings. See William G. Rich, 'The US Leans on Private Firms to Expose Foreign Hackers', 29 November 2018, Wired, https://www.wired.com/story/private-firms-do-government-dirty-work/.
[452] Anushka Kaushik, 'Public attribution and its scope and efficacy as a policy tool in cyberspace' (2019), https://www.orfonline.org/expert-speak/public-attribution-and-its-scope-and-efficacy-as-a-policy-tool-in-cyberspace-56826/. See also Cyber Operations Tracker, 'Operations by Country', https://www.cfr.org/cyber-operations/.
[453] Florian J. Egloff, 'Contested public attributions of cyber incidents and the role of academia' (2020), p. 56.
[454] The Five Eyes is an intelligence alliance established in 1946, consisting of the five mentioned states and their national security agencies. See e.g. Scarlet Kim, Paulina Perlin, 'Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance', 25 March 2019, https://www.lawfareblog.com/newly-disclosed-nsa-documents-shed-further-light-five-eyes-alliance.
[455] Anushka Kaushik, 'Public attribution and its scope and efficacy as a policy tool in cyberspace' (2019), https://www.orfonline.org/expert-speak/public-attribution-and-its-scope-and-efficacy-as-a-policy-tool-in-cyberspace-56826/

in cyber attribution can be identified. Firstly, the abovementioned states are some of the most technologically advanced in the world,[456] and therefore injured states might be apprehensive in giving excess publicity to cyber operations in fear of new cyber attacks, for instance, due to providing possible future perpetrators with useful information on potential flaws in their national cyber defense apparatus.[457] Correspondingly, drawing attention to cyber operations conducted against the state might undermine the public confidence in the state's ability to deter future cyber threats, and lead to public pressures on governments to strike back.[458]

Furthermore, victim states may not be aware that they have been the victim of a malicious *cyber* incident, and the Stuxnet virus offers an example of the latter, where Iran was not immediately aware of that its nuclear centrifuges were spinning out of control specifically due to a cyber operation.[459] In other words, a state's failure to identify, attribute or respond to a cyber operation may be due to evidential circumstances, where a state lacks the sufficient evidence to either identify that an attack has taken place or the evidence is inadequate in order to legally attribute the attack to any state.[460] Another reasoning behind a cautious approach to attributing cyber operations may also be of geopolitical nature. A state may fear that attributing certain cyber activity to another state may harm or hinder, for instance, ongoing diplomatic efforts or worry that the state can use the threat privately against another state to gain strategic advantages. In an attempt to deter a specific perpetrator without publicly attributing the cyber incident, the victim state can also have opted for a private dialogue with the attacking state to persuade or threaten the state to cease its unlawful behavior.[461] This was allegedly the case in 2016, when the Obama Administration attempted to privately communicate with Russia prior to publicly attributing the DNC hacks to the state.[462] Subsequently, it has been reported that the U.S.

---

[456] World Population Review, 'Most Technologically Advanced Countries 2020', https://worldpopulationreview.com/country-rankings/most-technologically-advanced-countries
[457] Efrony, Shany (n 102), p. 594.
[458] Ibid.
[459] Barrie Sander, 'The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations' (2019), p. 5.
[460] Ibid, p. 8.
[461] Kristen Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020), p. 552.
[462] Ibid; Greg Miller, Ellen Nakashima, Adam Entous, 'Obama's secret struggle to punish Russia for Putin's election assault', 23 June 2017, The Washington Post, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.d5ada09b5d4f.

Cyber Command is considering taking a similar approach against potential Russian attempts to interfere in the upcoming 2020 presidential election.[463] Finally, a lack of an effective response measure may also drive states to opt for remaining silent, as "[u]nless a nation is able to effectively redress a cyber intrusion, it can be harmful or self-defeating to publicize it, since public knowledge of loss and the failure to respond effectively invite more attacks."[464]

Moreover, failure to publicly explain whether or how international law applies in the cyber domain may further complicate effective state attribution. States may believe that international law is inadequate and thus be of the opinion that the limits of the available self-help remedies found under the law of state responsibility "may lead some States to conclude that there is little added utility in invoking international law in the cyber domain."[465] Put differently, states may not deem it necessary to claim that a violation of international law has occurred, since retorsion can is always an available response option and hence there is no need for a state to act within the limits of proportionality or notice.

Legal attribution refers to state's decision to attribute a certain conduct to the responsible state for the purpose of invoking state responsibility. From a cyber point of view, one of the most likely bases of attribution are that a state organ, such as the armed forces, launches a cyber operations, or that a non-state actor, for instance a hacktivist group of private cybersecurity company, conducted the internationally wrongful act upon the instructions or under the effective control of the state.[466] Hence the question at the heart of this subchapter is: how can a cyber operation be legally attributed to a state? This question is of outmost importance since most responses to cyber operations cannot be

[463] Ellen Nakashima, 'U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election' 25 December 2019, The Washington Post, https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html. See also Joan E. Greve, 'Steady drumbeat of misinformation': FBI chief warns of Russian interference in US elections', 17 September 2020, where Christopher Wray, the FBI director issued a warning about a Russian interference in the 2020 elections "…with a steady stream of misinformation aimed at undermining Democrat Joe Biden as well as sapping Americans' confidence in the election process." https://www.theguardian.com/us-news/2020/sep/17/misinformation-us-elections-2020-russia

[464] Jack Goldsmith, Stuart Russel, 'Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in its International Relations' (2018) p. 13, quoted in Sanders (n 459), p. 9.

[465] Sander (n 459), p. 9.

[466] Shany, Schmitt (n 435), p. 199.

deployed without attribution.[467] Consequently, the identification of the actor behind a cyber operation will determine the possible legal responses.[468]

4.2 Establishing cyber attribution

The law of attribution aims to identify and allocate responsibility for internationally wrongful acts. Accordingly, in lieu of wondering "who did it?", a more suitable question would be "who is to blame?"[469] The Draft Articles[470] lay out certain conditions that must be met in order for a conduct to be attributable to a state for the purposes of determining responsibility. As a starting point, conduct by state organs are always attributable to the state, whereas activities carried out by private individuals are not, unless a sufficient nexus between the private actors and the state can be determined. Rule 15 of the Tallinn Manual 2.0 states: "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."[471] Moreover, according to the Tallinn Manual 2.0, attribution to a state occurs in a number of circumstances, and states that the clearest case of attribution is when a state organ, for example the military or an intelligence agency, commits a wrongful act.[472] However, when it comes to cyber operations, it is not immediately clear whether it has been conducted by a state organ, since states rarely use their governmental agencies to conduct wrongful acts in cyberspace, and therefore various actors can be behind these cyber operations.[473]

---

[467] Delerue (n 48), p. 51.
[468] Delerue (n 48), p. 51.
[469] Jason Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks' (2012), p. 1.
[470] ILC Draft Articles, arts. 4-11.
[471] Tallinn Manual 2.0, Rule 15 – Attribution of cyber operations by State organs, p. 87.
[472] Ibid.
[473] Martha Finnemore, Duncan B. Hollis, 'Constructing Norms For Global Cybersecurity' (2016), p. 431. The use of state proxies in cyberspace is not uncommon. A proxy in the cyber context have been defined as "an intermediary that conducts or directly contributes to an offensive *cyber* operation that its enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effects." Valentin Weber, 'States and Their Proxies in Cyber Operations', 15 May 2018, Lawfare, https://www.lawfareblog.com/states-proxies-cyber-operations. States, notably the United States, Russia, China, Iran and Syria have been known to use them. An example of the latter would be the Syrian Electronic Army. (ibid). See also Tim Maurer, ''Proxies' and Cyberspace' (2016), Journal of Conflict & Security Law.

There is no reason to deny as a matter of principle the application of the attribution rules provided in the Draft Articles to conduct in cyberspace.[474] However, several characteristics of cyberspace make attribution particularly difficult.[475] The first challenge is to identify which computer or computers were used to prepare and carry out the cyber operation.[476] Computers obviously play the central role in the conducting of cyber operations, and computer identification is possible due to a computer's unique IP (Internet Protocol[477]) address and it can in some cases be traced to reveal the precise location of a computer.[478] However, "operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity."[479] Thus, in cyberspace, anonymity is easily achieved and maintained "not only in a personal sense, obscuring the identity of the person making keystrokes and clicks, but also in a technical sense, obscuring the location and identity of the cyber infrastructure from which harm originates."[480] The technical difficulty in attributing cyber operations often leave victim states in a difficult position where they are unable to trace the origin of the act, and thus preventing state responsibility from arising, which is worrisome since, attribution is a crucial element in avoiding impunity in cyberspace.[481]

Conversely, even if the computer behind the cyber operation is identified, it has a limited value for the purpose of attribution.[482] In other words, having a clear picture of the perpetrator is crucial, as cyber operations always involve a human perpetrator, attribution cannot be made unless the person operating the computer is identified as well.[483] This predicament has been named the "human machine gap":

> Even if an attacking computer can be located with sufficient certainty, what remains is the factor which commentators have called the 'human machine gap' or 'entry-point anonymity', the location of a computer rarely allows the definite conclusions regarding the identity of the

[474] Constantine Antonopoulos, 'State Responsibility in Cyberspace' (2015), p. 62.
[475] Tsagourias (n 57), p. 233.
[476] Chircop (n 267), p. 646; Jensen, Watts (n 1), p. 1555.
[477] Tallinn Manual 2.0, p. 566: "Internet Protocol (IP) Address: A unique identifier for a device on an IP network, including the Internet."
[478] Mauno Pihelgas, 'Back-Tracing and Anonymity in Cyberspace' (2013), p. 33; Chircop (n 267), p. 646.
[479] Henriksen (n 18), p. 341. Recall the example of the Russian cyber operations against the Olympic Games in South Korea in 2018.
[480] Jensen, Watts (n 1), p. 1558.
[481] Leandros Maglaras, 'Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures' (2019), p. 1.
[482] Chircop (n 267), p. 646.
[483] Ibid.

> individual operating the machine, and it is the latter's status that ultimately determines attribution pursuant to Articles 4 to 11 of the ILC Articles on State Responsibility.[484]

Even if the human perpetrator was identified, a sufficient legal nexus must be established between the actor and the state.[485] As Dionisio Anzilotti famously put it, "the activity of a State is nothing but the activity of individuals that the law imputes to the State."[486]

4.2.1 Attribution to a state

It is an obvious truism that states are inanimate abstract legal entities and cannot as such act themselves.[487] Draft Article 2 states that in order for an act or omission to amount to an internationally wrongful act, the unlawful conduct must be attributable to a state.[488] The actions of a state are carried out by either a state organ or a person or group acting on behalf of the state.[489] The conduct of a person or entity, despite not being organs of a state, but still empowered by internal law to exercise governmental functions are considered an act of state, given that they were acting in that capacity during that particular instance.[490] The latter also applies to *ultra vires* acts, where the state organ, person or entity exceeds its authority or disregards instructions.[491]

Hence, all cyber operations, even when programmed to happen automatically, were initially established by an individual, as were the procedures for initiation.[492] For the purpose of attribution, the law of state responsibility requires a link between the state and the person conducting an internationally wrongful act. The link encompasses the relation between the state and its *de jure* or *de facto* organs.[493] However, the concept of "organs

---

[484] Robin Geiss, Henning Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention' (2013), p. 625.
[485] Delerue (n 48), p. 72.
[486] Dionisio Anzilotti, 'Cours de droit international (1929) (Panthéon Assas, 1999), p. 469, quote taken from Zhxiong Huang, 'The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations' (2014), p. 42.
[487] See German Settlers in Poland, Advisory Opinion, [1923], PCIJ Rep. (ser. B) No. 6, para. 34: "States can act only by and through their agents and representatives."
[488] Draft Article 2 (a).
[489] Draft Articles 4-5. See also Settlers of German Origin in Poland, Advisory Opinion, 1923, P.C.I.J (ser. B) No. 6 (Sept. 10).
[490] Draft Articles, art. 5. The commentary gives an example of parastatal entities or private companies, which are not state organs in the sense of Draft Article 4 but are nonetheless entrusted with governmental tasks. Tallinn Manual 2.0, p. 87.
[491] Draft Articles, art. 7. Tallinn Manual 2.0, p. 89.
[492] Jensen (n 3), p. 15.
[493] Draft Articles, art.4; ICJ Genocide, para. 385.

of a state" in the law of state responsibility is broad.[494] All the persons or entities that have that status under domestic laws are state organs regardless of "whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State."[495] The logic behind the usage of such a broad meaning is to ensure that states do not escape international responsibility.[496] In other words, a state's organ need not be designated as such under domestic law in order for international state responsibility to emerge. The ICJ has taken a similar approach in its 2007 *Genocide* judgment, where the Court held that "persons, groups of persons or entities may, for purposes of international responsibility, be equated with State organs even it that status does not follow from internal law, provided that in fact the persons, groups or entities act in "complete dependence" on the State, of which they are ultimately merely the instrument."[497] In other words, the conduct of persons or entities *de facto* operating as an agent of the state will be attributable to that state.[498]

Acts of non-state actors may be attributable to a state, and Article 8 of the Draft Articles states that the "conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions or, or under the direction or control of, that State in carrying out the conduct."[499] For instance, a state may use a private company to conduct certain cyber activities and the company's conduct can under certain circumstances be attributable to the state. In other words, the state must have effective control[500] under which "for example, support for planning a cyber activity violating the territorial sovereignty and integrity of another State may amount to such a breach if the State is sufficiently

[494] Tallinn Manual 2.0, p. 87.
[495] Draft Articles, art. 4. Furthermore, there is no "distinction made at the level of principle between the acts of "superior" and "subordinate" officials, provided they are acting in their official capacity." See Art. 4(1), para. 7 of the commentary.
[496] Draft Articles, art. 4(2), para. 11 of the commentary. See also Tallinn Manual 2.0, p. 88.
[497] Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia), International Court of Justice (ICJ), 11 July 1996, para.392. See also Nicaragua judgment, paras. 109-110; Tallinn Manual 2.0, p. 88.
[498] ICJ Genocide, paras. 391-392; ICJ Nicaragua, para. 109.
[499] Draft Articles, art. 8.
[500] Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Servia and Montenegro) ICJ Reports 2007, paras. 403-403.

involved."[501] Hence a state must actively be involved in the planning and supervision of the activities in order for the non-state actor's conduct to be attributable to it.[502] Merely financing or providing equipment is not a sufficient nexus between the state and the non-state actor. That said, in a cyber context, the conduct of "hacktivists" or "patriotic hackers"[503] are not attributed to the state, nor is the expressing of support for such conduct enough to establish attribution.[504] An act is also attributable to the state if it acknowledges the conduct as its own.[505]

As established, the allocation of state responsibility for internationally wrongful acts in cyberspace, or any unlawful act under international law for that matter, requires proof of certain facts, such as a commission of an unlawful act, exposing the identity of the perpetrating entity, and determining the relationship between that entity and the state.[506] However, the ILC Draft Articles do not address evidentiary issues, stating in the commentary that "[q]uestions of evidence and proof of such a breach fall entirely outside the scope of the articles."[507] Furthermore, the Tallinn Manual 2.0 does not provide any clarification on the standards or methods of proof in relation to violations of cyber norms and concludes that they are to be "determined by the relevant forum."[508] Where does this leave malicious cyber operations? Put differently, is there a duty for states to provide factual evidence when attributing an internationally wrongful cyber operation to a state? Accordingly, what is the appropriate standard of proof, and for instance, how much proof must the victim state provide prior to initiating countermeasures?

[501] Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' (2013), p. 211; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 115.
[502] Tadic, para. 145.
[503] Hacktivists or political hackers usually carry out cyber activities in support of their agenda, be it politically or economically motivated. The most infamous hacktivist group is undoubtedly 'Anonymous', which has carried out thousands of cyber operations. See https://www.sciencedirect.com/topics/computer-science/hacktivists.
[504] Pirker (n 501), p. 211. However, in some circumstances the conduct of non-state actors may be adopted by a state as their own, see Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) ICJ Reports 1980, 3, para. 74.
[505] Draft Articles, art. 11; Tallinn Manual 2.0, Rule 17 (b).
[506] Yaël Ronen, 'Some Evidentiary Dimensions of Attributing Unlawful Cyber Operations to States' (2020), p. 1.
[507] Draft Articles, chapter. 3, commentary. 4, p. 54.
[508] Tallinn Manual 2.0, p. 83.

4.2.2 Cyber operations and evidentiary threshold

International law is not fully settled on the standard of proof that states must met when attributing an internationally wrongful act to a state.[509] The law in this area is mostly developed in relation to evidence to justify forcible self-defense in response to a prior armed attack.[510] However, how does this translate into cyberspace? As a point of departure, cyber attribution claims of are seldom followed by concrete evidence, despite an international consensus on that states should, whenever possible, reveal the basis for the attribution.[511] In particular, the 2015 UN GGE Report stated that "accusations of organizing and implementing wrongful acts brought against States should be substantiated."[512] However, as the rest of the norms of responsible state behavior proposed in the consensus report, they are of non-binding, voluntary nature and therefore do not constitute legal obligations.[513]

Regarding cyber operations, states have opined on this issue, and for instance the United States underlines that "the law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution."[514] Moreover, France has stated that while providing evidence helps legitimize the public attribution, international law does not require states to do so.[515] Furthermore, the Netherlands emphasizes that the burden of proof will vary depending on the events and the seriousness of the act that is considered to have violated international law.[516] The abovementioned state views echo the varying standards of proof taken by the ICJ, which "depend on the gravity of the breach and varies between a "fully conclusive" evidence standard for "charges of exceptional gravity", leaving "no room for reasonable doubt" to "proof at a high level of certainty appropriate to the seriousness of the allegation" for charges of lesser gravity."[517]

---

[509] Eichensehr (n 461), p. 559.
[510] Ibid.
[511] Shany, Schmitt (n 435), p. 213.
[512] 2015 UN GGE report, para. 28(f).
[513] Shany, Schmitt (n 435), p. 213.
[514] Brian J. Egan, 'Remarks on International Law and Stability in Cyberspace' (2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm; Roguski (n 328), p. 14.
[515] France, 'International Law Applied to Operations in Cyberspace', p. 11; Roguski (n 328), p. 14.
[516] The Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, p. 6; Roguski (n 328), p. 14.
[517] Roguski (n 328), p. 14.

However, when states do provide evidence when attributing cyber operations, they do so to a varying degree. For instance, when the United States attributed the Sony attack to North Korea, the evidence provided by the FBI press release was extremely restricted and underreported.[518] While some states seemed willing to accept the limited attribution evidence,[519] others publicly questioned the attribution and it sparked a widespread doubt.[520] Acknowledging the criticism, the FBI subsequently provided a second, slightly more detailed report, revealing more operational findings, such as the North Korean IP-addresses and code used in the hack.[521] In contrast, at the time of writing, one of the most detailed attribution claims is the Dutch investigation into the cyber operation against OPCW in The Hague in 2018, conducted by the GRU, where substantial evidence of the physical presence of the Russian government operatives in the Netherlands was established.[522]

Given the above, recent state practice seems to denote an emerging requirement to provide some form of evidence when attributing a cyber operation to another state. However, states that have opined explicitly on the evidentiary issues remain adamant that states are not required to provide evidence, even though it might be beneficial, and the latter "seems precisely designed to block the development of customary international law by denying the existence of one of the two requirements for custom."[523] In other words, despite the fact that states have revealed evidence when attributing malicious cyber operations might demonstrate consistent state practice, they have not done so out of a sense of legal obligation.[524] Even in the largest coordinated public attribution claim to

[518] Eichensehr (n 461), p. 563.
[519] UK, Foreign Secretary Philip Hammond, Foreign & Commonwealth Office Press Release, 'Foreign Secretary responds to FBI reports into cyber attacks on Sony Pictures', 19 December 2014, https://perma.cc/46BN-RG5P; Eichensehr (n 461), p. 563.
[520] Bruce Schneier, 'Did North Korea Really Attack Sony?', 22 December 2014, The Atlantic, https://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/; Joseph Marks, 'The Cybersecurity 202: The Sony hack ushered in a dangerous era in cyberspace', 27 November 2019, The Washington Post, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/27/the-cybersecurity-202-the-sony-hack-ushered-in-a-dangerous-era-in-cyberspace/5ddd716c602ff1181f264147/.
[521] Eichensehr (n 461), p. 564.
[522] Ibid.
[523] Ibid, p. 565.
[524] Ibid.

date, in which numerous states accused Russia for the cyber attacks against Georgia,[525] and while suggesting the existence of a strong basis for the allegations, no concrete evidence was publicly disclosed.[526]

[525] Premyslaw Roguski, 'Russian Cyber Attacks Against Georiga, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/;
[526] Sharngan Aravindakshan, 'Cyberattacks: a look at evidentiary thresholds in International Law' (2020), p. 5.

5. Responding to malicious state cyber operations

5.1 Remedies

First and foremost, under the duty of cessation, the perpetrating state must terminate its unlawful act.[527] The state must also offer the victim state assurances and guarantees of non-repetition.[528] States must make full reparation of the injury caused, whether material or moral, by the internationally wrongful act.[529] The purpose of reparations is to "wipe out" the consequences caused by the unlawful act and re-establish the situation "which would, in all probability, have existed if the act had not been committed."[530] It must be emphasized, that the meaning of reparations is not to re-establish the *status quo* which had existed prior to the violation occurring, but rather re-establishing the situation which in all likelihood would have existed had the wrongful act not occured. The forms of reparation are restitution, compensation, and satisfaction.[531]

As was shown above, states have begun demonstrating an increasing readiness and political willingness to attribute malicious cyber operations to the states of origin.[532] The legal standards for attribution are becoming more transparent and while no legal requirement to provide evidence to support the attribution claims exists, states are doing so and with growing levels of confidence and details.[533] States have also started seeking legal options to impose costs on states responsible for malicious cyber operations and denounce their actions.[534] State responses to have thus far been limited to retorsion, such as sanctions, indictments, and publicity.[535] For instance, in July 2020, the European Union imposed its first ever sanctions against six individuals and three entities responsible for the cyber operations against OPCW, and involvement in WannaCry, NotPetya and Operation Cloud Hopper.[536] The sanctions included a travel ban and the freezing of assets

[527] Draft Articles, art. 30 (a); Tallinn Manual 2.0, p. 142.
[528] Draft Articles, art. 30 (b); Tallinn Manual 2.0, p. 142.
[529] Draft Articles, art. 31 (1); Draft Articles, art. 31 (2); Tallinn Manual 2.0, p. 144.
[530] PCIJ, Factory at Chorzów, (Germany v. Poland), 13 September 1928, p. 47.
[531] Draft Articles, art. 34.
[532] NATO CCDCoE, 'Trends in international law for cyberspace' (2019), p. 2, available at https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf; Moynihan (n 4), p. 4.
[533] NATO CCDCoE, 'Trends in international law for cyberspace' (2019), p. 2, available at https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf
[534] Ibid.
[535] Ibid.
[536] European Council, Press release, 'EU imposes the first ever sanctions against cyber-attacks', 30 July 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-

and were taken against two Chinese citizens, four Russians, and three organizations from China, Russia, and North Korea.[537] As for indictments, in 2018, the United States charged seven Russian GRU officers for their involvement in the hacking of the World Anti-Doping Agency (WADA),[538] as well as the cyber operation against OPCW.[539] As mentioned above, many cyber operations are covert in nature but when the Netherlands discovered the Russian cyber operations against OPCW, it publicly revealed the intricate details of the operation, such as the timeline of the events and the equipment used, thus giving it publicity.[540]

In other words, the majority of state responses taken against malicious cyber operations have been "measures of discourtesy or unfriendliness vis-à-vis another State".[541] Subsequently, there are no confirmed uses of countermeasures against state cyber operations as prescribed under the law of state responsibility.[542] To date, not a single cyber operation has resulted in the use of kinetic or cybernetic force as a response option.[543] However, NATO Secretary General, Jens Stoltenberg, has stated that "[a] serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all."[544] NATO has in fact recognized cyberspace as "a domain of

---

sanctions-against-cyber-attacks/. During Operation Cloud Hopper, eight of the world's biggest technology service provides, including IBM and Fujitsu, were hacked by Chinese 'cyber spies' during several years. The hacking campaign impacted organizations in North America, South America, Asia and Europe, including Finland. Jack Stubbs, Joseph Menn, Christopher Bing, 'Inside the West's failed fight against China's 'Cloud Hopper' hackers, Reuters, 26 June 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/; Yle Uutiset, 'Suomi on ollut tietoverkkohyökkäyksen kohteena', 5 April 2017, https://yle.fi/uutiset/3-9548424.

[537] Axel Scroxton, 'EU sanctions China and Russia over cyber attacks', 31 July 2020, Computer Weekly, https://www.computerweekly.com/news/252486952/EU-sanctions-China-and-Russia-over-cyber-attacks.

[538] WADA Confirms Attack by Russian Cyber Espionage Group, 13 September 2016, https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group.

[539] United States, Department of Justice, 'U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations', 4 October 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

[540] The Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', 4 October 2018, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw; NATO CCDCoE, 'Trends in international law for cyberspace' (2019), p. 5, available at https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf.

[541] Tom Ruys, 'Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework' (2016), p. 5.

[542] NATO CCDCoE, 'Trends in international law for cyberspace' (2019), p. 2, available at https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf; Draft Articles, art. 22.

[543] Efrony, Shany (n 102) p. 586.

[544] NATO, 'NATO will defend itself', 27 August 2019, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en. Article 5 of the NATO Treaty:

operations in which NATO must defend itself as effectively as it does in the air, on land and at sea."[545] Stoltenberg specifically referred to WannaCry, stating that such an attack of such calibre could prompt a collective defence commitment, in other words lead the military alliance to react with force.[546]

Given the above, as states continue to employ cyber tools to commit malicious activities in cyberspace, countermeasures might come to play an increasingly important role in interstate relations.[547] Understanding when, how and under which circumstances states may lawfully employ countermeasures is paramount for state conduct in cyberspace, not merely for victim states to recognize their response options, but also for states to anticipate possible responses their malevolent cyber conduct may prompt from other states.[548] However, determining what constitutes a proportionate response to malicious cyber activity is not straightforward. The covert nature of state cyber operations and the fact that they may build up slowly and incrementally may lead to difficulties.[549] More specifically, the exact nature and scale of effects can be estimated at a late stage, if at all.[550] For example, the responses taken by the U.S. in relation to the DNC Hacks was not well received by all: "The punishment did not fit the crime. Russia violated our sovereignty, meddling in one of our most sacred acts as a democracy – electing our president. The Kremlin should have paid a much higher price for that attack."[551]

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area." Article 5 has not been invoked since the 9/11 terror attacks on the US in 2001, BBC News, 'Nato: Cyber-attack on one nation is attack on all', 27 August 2019, https://www.bbc.com/news/technology-49488614.

[545] NATO, Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, 9 July 2016, para.70, https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber.

[546] Gareth Corfield, 'WannaCry ransomware attack on NHS could have triggered NATO reaction, says German cybergeneral', The Register, 3 February 2020, https://www.theregister.com/2020/02/03/wannacry_nato_response/.

[547] Ashley Deeks, 'Defend Forward and Cyber Countermeasures', 12 August 2020, Lawfare, https://www.lawfareblog.com/defend-forward-and-cyber-countermeasures.

[548] Ibid.

[549] Pirker (n 501), p. 213.

[550] Ibid.

[551] Michael McFaul, former U.S. ambassador to Russia, quoted in Greg Miller, Ellen Nakashima, Adam Entous, 'Obama's secret struggle to punish Russia for Putin's election assault', 23 June 2017, the Washington Post, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.d5ada09b5d4f.

5.2 Retorsion

If a cyber operation does not qualify as an internationally wrongful act, an injured state is not left without available response options. First and foremost, countermeasures must be distinguished from retorsion. While they are both lawful response measures for cyber operations falling below the level of armed attack (thus excluding the use of self-defense as a response), the distinguishing factor is that countermeasures would otherwise be in violation of international law without the prior commission of a breach by the responsible state, whereas acts of retorsion are lawful but unfriendly acts taken against the violating state, irrespective of the latter state's conduct.[552] In other words, while retorsions may indeed be taken as a response to an internationally wrongful act, it need not be the case.[553]

In legal debates surrounding possible state responses to malicious cyber operations, acts of retorsion have usually not been discussed in great length.[554] Only a few states, Australia, the Netherlands and the United States, have thus far specifically referred to retorsion as a response option to malicious cyber activities.[555] According to the Netherlands, retorsion is always an available response option to unlawful conduct by another state, since it constitutes a lawful exercise a state's sovereign rights.[556] Retorsion is regarded as being both flexible and limited; flexible in the sense that unlike other response options, it has relatively few operational requirements, and limited due to the fact that the actions taken must not themselves constitute a breach of international law.[557] Consequently, international law does not require retorsions to be proportionate nor do they need to be temporary or reversible, as is the case with countermeasures.

That said, which actions qualify as retorsion in cyberspace? The most frequently quoted examples include, *inter alia*, ending diplomatic relations, expelling aliens, as well as

[552] Draft Articles, ch. II, para. 3 of commentary; Michael Schmitt, 'Cyber Responses "By The Numbers" in International Law', 4 August 2015, EJIL: Talk!, https://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/; Tallinn Manual 2.0, p. 112.
[553] Ruys (n 541), p. 5.
[554] Jeff Kossef, 'Retorsion as a Response to Ongoing Malign Cyber Operations' (2020), p. 10.
[555] Roguski (n 328), p. 18.
[556] Netherlands Minister of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace (July 5, 2019), Appendix: International Law in Cyberspace, https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf, p. 7; Kossef (n 554), p. 10.
[557] Kossef (n 554), p. 10.

economic sanctions and travel restrictions.[558] An illustrative example is the Sony Hack, when on 24 December 2014, the North Korean Internet service was shut down for nine hours, following another two days of network interruptions. It is widely speculated that the shutting down of the Internet was a covert reaction on the Sony hacks, albeit never confirmed by the United States.[559] In January 2015, the United States imposed additional sanctions on North Korea in response to the nation's "ongoing provocative, destabilizing, and repressive actions and policies, particularly its destructive and coercive cyber attack on Sony Pictures Entertainment."[560] Actions were taken against three North Korean governmental organisations, including the country's intelligence agency, as well as ten state officials.[561] Such responses involve, to varying degrees, measures of discourtesy, but do not violate international legal principles and hence qualify as acts of retorsion.[562] Despite having geopolitical implications, it is "safe to assume that the recourse to actions which do not violate international obligations is largely unproblematic."[563]

5.3 Countermeasures

States bear responsibility for their internationally wrongful acts pursuant to the law of state responsibility. Countermeasures are a remedial measure consisting of state actions, or omissions, taken against another state as a response to a prior violation of an obligation owed to the state. Since countermeasures are conducted in order to compel or convince the perpetrating state to discontinue the internationally wrongful act, they amount to a legal means of self-help.[564] The requirements for countermeasures apply in cyberspace, as they must be aimed at the responsible state,[565] may never be taken for punitive purposes and must only be used to inducing compliance by the perpetrating state with its

[558] Malcom N. Shawn, 'International Law' (2017), p. 859, quoted in Kossef (n 554), p. 17.
[559] BBC News, 'Why did North Korea's internet go down?', 23 December 2014, https://www.bbc.com/news/world-asia-30586940.
[560] The White House, Office Press Secretary, 'Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea"', 2 January 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.
[561] Dan Roberts, 'Obama imposes new sanctions against North Korea in response to Sony hack', 2 January 2015, The Guardian, https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.
[562] Kossef (n 554), p. 18.
[563] Roguski (n 328), p. 18.
[564] Schmitt (n 37), p. 701; Tallinn Manual 2.0, p. 113.
[565] For instance, in the *Gabčikovo–Nagymaros Project* case, the ICJ clearly states that countermeasures "must be taken in response to a previous international wrongful act of another State and must be directed against that State." Gabčikovo–Nagymaros Project (Hungary v. Slovakia), ICJ Judgement, 1997, para. 83.

international obligations, therefore restoring the *status quo*.[566] The countermeasures do not specifically need to target state organs or state infrastructure, although the state itself needs to be the object of the countermeasure.[567]

Draft Articles 22 and 49-52 set out the parameters of countermeasures and a state is entitled to react as long as the requirements applicable to countermeasures are met. First and foremost, countermeasures may not under any circumstances be designed to punish the perpetrating state, but rather to push the state to comply with its legal obligations and cease the unlawful activity. Countermeasures may not violate the prohibition on the use of force.[568] In the case of conduct falling below the level of an armed attack, two positions have emerged; the prevailing view is that a state may only resort to non-military countermeasures, whereas a minority opinion has been put forward by Judge Simma in the Oil Platforms case, where he suggests that states may resort to force when reacting to activities falling below the threshold of an armed attack.[569] It is furthermore important to keep in mind that countermeasures need not be in kind, nor violate the same norm that was priorly breached by the responsible state,[570] nor do they need to be conducted in cyberspace: "A State may be entitled to take countermeasures, whether cyber in nature of not, in response to a breach of an international legal obligation that it is owed by another State."[571] Echoing the latter, France, the United Kingdom and the United States have specifically opined that countermeasures taken in response to a cyber operations need not be limited to measures in kind, and they may resort to non-cyber countermeasures.[572] Whereas countermeasures are taken to terminate an ongoing unlawful act and may not be taken in response to an act that has ended, in the case of WannaCry, as the attacks are no

[566] Pirker (n 501), p. 212.
[567] Tallinn Manual 2.0, p. 112-113.
[568] Draft Articles, art. 49.
[569] Pirker (n 501), p. 213; Oil Platforms (Islamic Republic of Iran v. United States of America) ICJ Reports, 2003, 161, separate opinion of Jugde Simma, para. 12: "What we see in such instances is an unlawful use of force "short of" an armed attack ("aggression armée") within the meaning of Article 51, as indeed "the most grave form of the use of force". Against such smaller-scale use of force, defensive action – by force also "short of" Article 51 – is to be regarded as lawful."
[570] Michael Schmitt, 'Cyber Responses "By The Numbers" in International Law', 4 August 2015, EJIL: Talk!, https://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/.
[571] Tallinn Manual 2.0, Rule 20 – Countermeasures (general principle), p. 111.
[572] Roguski (n 328), p. 18.

longer ongoing, the countermeasures are only available in order to compel North Korea to make full reparations, such as providing compensation for the injured states.[573]

First, prior to resorting to countermeasures, the injured state must call upon the responsible state to cease its unlawful activity.[574] Accordingly, due to the nature of countermeasures, the responsible state must be made aware of that the countermeasures have been taken in response to its misconduct. For potential negotiations to take place, the victim state must notify that it has decided to take countermeasures against the responsible state prior to launching them.[575] Furthermore, the countermeasures must be proportionate, taking into account the gravity of the previous offence.[576] If the countermeasures are not proportionate to the injury caused by the internationally wrongful act, they amount to reprisals which are prohibited under international law, and therefore the wrongfulness of the countermeasure is not precluded.

Judicial decisions, doctrine and state practice confirm the legality of countermeasures[577] and states have also shown a willingness to adapt the use of countermeasures in the cyber context.[578] For instance, regarding the requirement of notice, France has stated that the injured state may, in certain circumstances, deviate from the obligation of a prior notice, in order to protect its rights.[579] France further states that adopting urgent countermeasures is deemed more appropriate in cyberspace due to the classified nature of cyber operations and the difficulties in tracing the origin of the attacks.[580] This position was echoed by the Netherlands, stating that states must in general call upon the responsible state to terminate its unlawful acts, unless urgent countermeasures are necessary to safeguard the rights of the injured state.[581] However, the most noteworthy position is that of the United Kingdom, claiming that the country "would not agree that we are always legally obliged to give

[573] Michael Schmitt, Sean Fahey, 'WannaCry and the International Law of Cyberspace', 22 December2017, Just Security, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/; Tallinn Manual 2.0, p. 118.
[574] Draft Articles, art. 52 1 (a); Gabčikovo–Nagymaros Project (Hungary v. Slovakia), ICJ Judgement, 1997, para. 84.
[575] Draft Articles, art. 52 1 (b); Tallinn Manual 2.0, p. 120.
[576] Gabčikovo–Nagymaros Project (Hungary v. Slovakia), ICJ Judgement, 1997, para. 85; Tallinn Manual 2.0, p. 127.
[577] Draft Articles, art. 22, para. 2 of commentary.
[578] Schmitt (n 94), p. 43.
[579] France, 'International Law Applied To Operations in Cyberspace' p. 8; Schmitt (n 94), p. 45.
[580] Ibid.
[581] Schmitt (n 94), p. 45.

prior notification … it could not be right for international law to require a countermeasure to expose highly sensitive capabilities."[582] The position is notable and stands out due to the fact that it highlights the preservation of the highly classified state cyber capabilities and a justification for not providing notice, whereas the beforementioned statements underscore the impracticality of the latter.[583]

The question of collective countermeasures has also arisen.[584] Estonia was the first state to publicly address the issue of collective countermeasures in relation to malicious cyber operations, in fact stressing the importance. Accordingly, Estonia has stated that states "which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation."[585] The only open contradiction to the statement has been provided by France,[586]and the use of collective countermeasures remains unresolved at the time of writing.

5.4 Plea of necessity

Countermeasures must also be differentiated from actions taken on a plea of necessity.[587] They differ in three different ways: first, there is no requirement of an underlying internationally wrongful act prior to invoking a plea of necessity; second, the responsible actor behind the incident does not need to be identified; lastly, invoking a plea of necessity must be a last resort, where the situation is dire and the essential interests of a state are in imminent danger.[588] Contrary to countermeasures, the mere wrongfulness of an action is not sufficient to trigger the response option of necessity. From a cyber point of view, a

[582] Jeremy Wright, 'Cyber and International Law in the 21st Century', 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Schmitt (n 94), p. 45.
[583] Schmitt (n 94), p. 45.
[584] See generally e.g. Samuli Haataja, 'Cyber Operations and Collective Countermeasures under International Law' (2020).
[585] President of the Republic at the opening of CyCon 2019, 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html
[586] France, 'International Law Applied To Operations in Cyberspace' p. 7: "Collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's right." However, the French position does not clarify the reasoning behind this stance. Schmitt (n 94), p. 45.
[587] Schmitt (n 37), p. 702.
[588] Ibid; Tallinn Manual 2.0, p. 135.

probable scenario of a state invoking the plea of necessity would be a cyber operation threatening the operational functionality of critical infrastructure.[589] Accordingly, as a last resort, a state could decide to partially shut down its cyber infrastructure as a protective response to a cyber operation endangering the essential interests of the state, which could have effects in other state's cyber systems.[590] It is important to bear in mind that the plea of necessity and the actions taken are aimed at the danger itself and not the responsible state, and therefore, attribution is not crucial in cases where, for instance "action is taken against hijacked computer systems without knowing or being able to reach the command and control computer."[591]

Despite the precise nature and scope of a plea of necessity remaining controversial, the International Group of Experts (IGE) agreed that as a general matter, the plea of necessity is customary in nature and is thus applicable to cyber contexts.[592] However, two points should be taken into consideration. First, as was mentioned above, in order to invoke a plea of necessity, certain restrictive conditions must be met.[593] The acts undertaken must be "the only way for the State to safeguard an essential interest against a grave and imminent peril; and [should] not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole."[594] Restated, acting on basis of necessity is only permitted when a state's essential interests are severly imperilled.[595] Conversely, what constitutes an "essential interest" is contested, and no commonly accepted definition of the term exists.[596] What is considered to be an essential interest undoubtedly varies from state to state, and is therefore contextual.[597] In the cyber context, due to the modern society's heavy reliance on ICTs, one could speak of critical cyber infrastructure as being an essential interest of a state. Accordingly, with regard to WannaCry and its damaging effects on hospitals and medical facilitates in the United Kingdom, the attack can be seen as having damaged an "essential interest" of the state. However, since WannaCry has ended and is no longer ongoing, the

[589] Schmitt (n 37), p. 703.
[590] Pirker (n 501), p. 214.
[591] Ibid.
[592] Tallinn Manual 2.0, p. 135.
[593] Pirker (n 501), p. 214.
[594] Draft Articles, art. 25 (a), (b).
[595] Tallinn Manual 2.0, p. 135.
[596] Ibid; Draft Articles, art. 25, para. 15 of commentary.
[597] Tallinn Manual 2.0, p. 135.

plea of necessity would not be available since the purpose is to terminate the malicious act.[598]

[598] Michael Schmitt, Sean Fahey, 'WannaCry and the International Law of Cyberspace', 22 December2017, Just Security, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/; Tallinn Manual 2.0, p. 139.

6. Conclusion

State affiliated cyber operations have become increasingly more sophisticated and have demonstrated that damage to critical infrastructure has become the new normal.[599] However, states conducting or supporting cyber operations have consistently denied the accusations or refused to comment and therefore remained silent on the matter.[600] Moreover, the increase in accusations are of great concern, since the accusers almost always fail to invoke international law, let alone assess whether or not the state behavior complies with its rules. State sponsored cyber operations are merely labelled as, for instance, violations of international norms or as flagrant violations of international law.[601] For state responsibility to arise, the conduct must be unlawful, and referring to a malicious cyber operation using terms without a legal connotation results in even greater difficulties in ending impunity in cyberspace. The absence of references to international law provisions in current attribution claims further obstructs its effective application to cyber scenarios. By refraining to legally characterize cyber operations, that is clearly providing a reference to what rule of international law has been allegedly been violated, states are missing the opportunity to develop international law, which ultimately encourages further malevolent cyber activities by states. Thus far, the majority of public attribution claims have remained at a political and technical level, with states refraining from addressing legal attribution, which in turn would reveal *opinio juris* on the matter. In other words, no state has specifically claimed that a cyber operation conducted against them would have amounted to an internationally wrongful act. It has therefore been suggested by some, that attribution could be seen more as a "naming-and-shaming tool of deterrence" rather than being a basis of invoking state responsibility.[602]

The main aim of the thesis was to analyse how cyber operations may constitute internationally wrongful acts by violating state sovereignty, as well as the prohibition of intervention into the internal or external affairs of another state, for which injured states may seek reparations or react through proportionate countermeasures. It was held that

[599] Piret Pernik, 'Responding to "the Most Destructive and Costly Cyberattack in History", International Centre for Defence and Security, February 28, 2018, https://icds.ee/responding-to-the-most-destructive-and-costly-cyberattack-in-history/
[600] Martha Finnemore, Duncan B. Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' 2019, p. 2.
[601] Ibid.
[602] Väljataga (n 93), p. 17.

cyber operations that cause damage, injury, or a semi-permanent loss of functionality of another state's governmental cyber infrastructure or private entities amount to a violation of that state's territorial sovereignty. A violation of sovereignty can also occur when a cyber operation interferes with or usurps inherently governmental functions, for instance targeting an electronic voting system used in a state election, thereby affecting the voting process and potentially the whole outcome of the election.. Furthermore, cyber operations that interfere with another state's *domain reservé* in order to coerce or compel the state into certain behavior would amount to an unlawful intervention. In the case of WannaCry, the operation did not violate the territorial integrity of the affected states but may be seen as having interfered with inherently governmental functions, thus amounting to an internationally wrongful act. WannaCry did not qualify as unlawful intervention seen as it failed to satisfy the element of coercion. The majority of state responses have consisted of retorsion, such as the expulsion of diplomats or ordering of economic sanctions against the responsible state. To date, no known instances of countermeasures, whether in cyberspace or in the kinetic world, have been observed in relation to a malicious cyber operation.

Differing views on the extent to which sovereignty is a legally binding rule that can be violated in the context of cyberspace have surfaced. Recent state practice shows that states have divided themselves into two camps, one favoring a sovereignty "as a rule" approach, and one assenting to a "sovereignty as a principle" approach. Recent positions of states, (Austria, Czech Republic, and Finland) are important contributions to the ongoing debate regarding the status of sovereignty and the state practice and *opinio juris* in the cyber domain. Another important aspect of these statements shows that not only major cyber powers contribute to the discission, and therefore showing example for other states to follow.

As became apparent, navigating the murky waters of cyberspace is by no means any easy task. While it is no longer seriously contested that international law applies to cyberspace, many aspects of the application remain unsettled and states cannot seem to agree on specifics. It can be held that two distinct problems have risen with the current application of international law to cyberspace. Firstly, states might find themselves in situations where it is unclear which rules apply to state cyber operations, or secondly, situations where states assume a certain rule to apply despite the outline and meaning being unclear

or disputed.[603] However, states have in fact shown an uneven interest in fostering the legal debate in cyberspace. Notwithstanding the recent proliferation in national views on the applicability of international law to cyberspace, the statements are nonetheless overshadowed by the number of states that have not done so.[604] Likeminded Western states have advocated that cyberspace ought to be regulated by extant international law but failing to answer the "million-dollar question" of how these existing legal frameworks are to be interpreted in the cyber context. In contrast, the Russia and China are pushing for a specific multilateral cyber treaty, while the creation of a specific cyber treaty has been met with opposition. The primary reasoning behind the rejection of the idea is that the instrument would take years to negotiate, while ultimately not solving the question of how it would apply to cyberspace.[605]

An analogy has been drawn between cyber regulation and "the law of the horse":

> Isn't this just "the law of the horse?" I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile.[606]

Hence, with the future in mind, an important question raised is whether extant international law is sufficient to regulate state behavior in cyberspace, or whether a separate cyber regime would be more suitable; for some, the answer is not to develop a new set of legal rules, that is a law of the horse for cyberspace, but to further clarify and articulate how existing international legal rules can and should be applied to cyber operations.[607] Further, a "wait and see" approach has emerged, according to which the international community should simply allow states to interact for a sufficient amount of time, thus eventually leading to the materialization of state practice and *opinio juris*.[608] However, on the other end of the spectrum, others are of the opinion that the law of the horse is paramount, and advocates of this approach deem it essential for specific

[603] Hollis (n 19), p. 4.
[604] Shany, Schmitt (n 435), p. 198.
[605] Schmitt (n 94), p. 35.
[606] Frank Easterbrook, 'Cyberspace and the Law of the Horse' (1996), p. 208.
[607] Duncan B. Hollis, 'Four Challenges for International Law and Cyberspace: Sartre, Baby Carriages, Horses, and Simon& Garfunkel Part 2', 7 May 2019, Council on Foreign Relations, https://www.cfr.org/blog/four-challenges-international-law-and-cyberspace-sartre-baby-carriages-horses-and-simon-0.
[608] Ibid.

international legal rules for cyberspace to be established.[609] In their view, a specifically tailored regime would better regulate the potential threats emanating from cyberspace.

Indeed, the application of existing legal regimes to new technologies is not an easy task and it has certainly been the case with information technology and cyberspace.[610]. As has been noted by the ILC "failure to react over time to a practice may serve as evidence of acceptance as law (*opinio juris*), provided that States were in a position to react and the circumstances called for some reaction."[611] However, allowing states that possess the most advanced technological capabilities "to do anything they want in cyberspace and thereby create a new rule of customary international law without protest from the other states runs the risk of giving the former states a monopoly of cyberspace law-making to serve their own interests."[612] It would be both unrealistic and undesirable to adopt a "wait and see" approach, since state practice in cyberspace is mostly classified and publicly unavailable. Therefore, it would be unreasonable to require states to opine on any new rules concerning cyberspace without having full disclosure of the situation. To this end, new law does not need to be made, and it has been deemed unlikely that new norms cyber specific customary international law will crystalize in the near future.[613] The crystallization of new customary international law requires consistent, widespread state practice that develops over time and a sense of legal obligation by which state adhere or refrain from certain conduct. A clear obstacle in in cyberspace is that much of state cyber operations are conducted in secrecy, and therefore highly classified resulting in a considerable number of incidences not reaching the public eye, let alone the legal community. Understandably, invisible state practice cannot contribute to the formation of new customary norms. Complicating the matter even further is the fact that scarceness of states condemning malicious cyber operations as violations of international law. It is also difficult to tell, given the existing state practice and *opinio juris*, whether states are refraining from conducting malicious cyber activity out of a sense of legal obligation or mere self-interest. States are seemingly not willing to get their hands tied by agreeing to

[609] Ibid.
[610] Gary Corn, 'Tallinn Manual 2.0 – Advancing the Conversation' 15 February 2017, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.
[611] International Law Commission, 'Draft conclusions on identification of customary international law' (2018), para. 10 (3).
[612] Kittichaisaree (n 82), p. 22.
[613] Schmitt (n 94), p. 35.

certain principles and therefore also limiting their own cyber activity. The gray zone in which numerous states operate combined with the prevailing ambiguity surrounding the application of international law to cyberspace can be favorable to states.[614]

The debate surrounding the precise manner in which international law ought to be applied in cyberspace will surely remain thorny for some time to come. Efforts should be focused on finding a common ground for the interpretation of extant international law. As it is highly unlikely that states will stop conducting malicious cyber operations, it is therefore essential for states to continue to publicly issue their understandings of the relevant international legal issues concerning malicious cyber activities in cyberspace, even though consensus may not realistically be achieved in the short term.[615]

[614] Michael Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017), p. 3; Schmitt (n 94), p. 38.
[615] Przemyslaw Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', Just Security, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

SVENSK SAMMANFATTNING – SWEDISH SUMMARY

FOLKRÄTTSSTRIDIGA HANDLINGAR I CYBERRYMDEN – TILLSKRIVANDET AV STATSANSVAR FÖR FREDSTIDA CYBEROPERATIONER

Att dagens samhälle är beroende av informationsteknik är inte någon ny företeelse – allt från statsapparaturens och militärens agerande till privata individers vardagstjänster utförs i den så kallade cyberrymden, eller cyberdomänen. Många kritiska samhällsfunktioner, speciellt informations- och styrsystem (SCADA) är därmed beroende av cyberrymden och internet. Cyberrymden är uppgjord av en gränsöverskridande informationsmiljö som består av sammanlänkade IT-infrastrukturer, såsom intranät, telekommunikationssystem men även geografiskt bundna, fysiska komponenter som datorer och hårdskivor. Med cyberoperationer avses handlingar som utförs i eller genom cyberrymden för att uppnå särskilda mål och innefattar t.ex. dataintrång, överbelastningsattacker (DDoS), virus och sabotageprogram.

Cyberrymden har ofta beskrivits som en teknologisk vilda västern utan folkrättslig reglering där såväl stater som icke-statliga aktörer genomför cyberoperationer av varierande form och skala. Diskussionen kring cyberoperationer har länge varit av humanitärrättslig karaktär, där debatten i det internationella samfundet i stor utsträckning präglats av frågor kring bl.a. regleringen av cyberkrigföring. Dock utsätts stater dagligen för cyberoperationer som varken uppnår tröskeln för väpnat angrepp eller utförs inom ramen för en pågående väpnad konflikt.

Den amerikanska tankesmedjan CFR (Council on Foreign Relations) har sedan 2005 upprätthållit en databas över cyberoperationer som misstänks vara statssponsorerade, och under det senaste årtiondet har närmare trettio stater, bland dem USA, Storbritannien, Ryssland, Kina, Nordkorea och Iran, anklagats för att ha utfört eller understött statliga cyberoperationer. Det uppskattas även att långt över 100 stater har utvecklat förmågan att utföra offensiva cyberoperationer. Ett dagsaktuellt exempel är cyberoperationer mot Världshälsoorganisationen WHO:s databaser utförda av statssponsorerade hackare från Iran. WHO har även rapporterat en femfaldig ökning av offensiva cyberangrepp mot hälsomyndigheter världen över sedan början av coronapandemin.

Utgående från en rättsdogmatisk analys granskas i avhandlingen statsansvarsreglernas tillämpbarhet i cyberrymden och avsikten är således att påvisa hur cyberoperationer kan utgöra folkrättsstridiga handlingar som aktualiserar statsansvar. Cyberoperationer per se är inte förbjudna i folkrättslig bemärkelse. Avsaknaden av traktaträtt som specifikt reglerar cyberoperationer lyfter fram internationella sedvanerättens centrala betydelse gällande staters cyber aktiviteter. Sedvanerätten består av statspraxis och opinio juris. Statspraxis utgörs av staters agerande medan opinio juris avser en stats rättsliga övertygelse att den är bunden av en specifik sedvänja. En betydande del av staters agerande i cyberrymden är dold från allmänheten vilket försvårar avgörandet av växande statspraxis eller förekomsten av opinio juris.

Fokuset är därmed på hur cyberoperationer kan kränka suveränitetsprincipen samt bryta mot principen om icke-inblandning i en stats interna angelägenheter. Som utgångspunkt används statsansvarsrätten som är kodifierad i FN:s folkrättskommissions (ILC) artiklar om statsansvar för folkrättsstridiga handlingar, som har en stark sedvanerättslig ställning i folkrätten. Som en betydande sekundärkälla används den s.k. Tallinnmanualen 2.0, som inte är en officiell mellanstatlig överenskommelse, utan ett omfattande akademiskt samt auktoritativt verk författat av en grupp självständiga experter (IGE) och folkrättsjurister i ett försök att kodifiera gällande rätt inom cyberdomänen. Som en betydande fallstudie i avhandlingen används utpressningsviruset WannaCry, som enligt Europol utgör en av de största cyberattacker genom tiderna. I maj 2017 angrep WannaCry datorer med en föråldrad version av operativsystemet Microsoft Windows. Viruset krypterade data på de infekterade datorerna och krävde en lösensumma i kryptovalutan Bitcoin. WannaCry lamslog omkring 200 000 datorer i åtminstone 150 länder världen över. Dock var det Storbritannien som drabbades hårdast då stora delar av landets sjukvårdssystem (NHS) paralyserades; ambulanser omdirigerades och tusentals operationer samt läkarbesök ställdes in då sjukvårdspersonalen inte hade tillgång till patientdata.

Stater har folkrättsliga rättigheter och skyldigheter gentemot andra stater och det internationella samfundet i dess helhet. Stater har suverän kontroll över cyberinfrastruktur samt cyberverksamhet som begås på deras territorium och har därmed en skyldighet att förhindra att deras cyberinfrastruktur används för att skada en annan stat.

För att statsansvar ska aktualiseras bör en folkrättsstridig handling ha begåtts som kan tillskrivas staten och grunder för ansvarsfrihet bör ha uteslutits. Kränkningar av suveränitetsprincipen framstår enligt Tallinnmanualen 2.0 som de mest sannolika folkrättsöverträdelser i cyberdomänen, trots meningsskiljaktigheter stater emellan. För att en cyberoperation ska anses bryta mot suveränitetsprincipen bör den utgöra en kränkning av statens territoriella integritet eller inkräkta på statens myndighetsövande, t.ex. ordnandet av val eller upprättandet av diplomatiska förbindelser. Därutöver måste cyberoperationen orsaka fysisk skada eller funktionalitetsstörningar. WannaCry-viruset orsakade inga fysiska skador i de drabbade länderna, men kan dock anses ha inkräktat på staters myndighetsövning då b.la. viruset lamslog det ryska inrikesministeriets datorsystem.

Cyberoperationer kan kränka den sedvanerättsliga principen om non-intervention i en annan stats interna angelägenheter. En otillåten inblandning äger rum då en stat i syfte att tvinga en annan stat till ett visst beteende inkräktar på statens interna eller externa angelägenheter (domain réservé). Närmare bestämt måste handlingen uppfylla två förutsättningar för att klassas som intervention; den bör inkräkta på en stats rätt till maktutövning och omfatta ett visst mått av tvång, dvs. tvinga staten att handla på ett ofrivilligt sätt eller avstå från en viss handlingslinje. Ett ökänt exempel på cyberoperationer som kvalificerats som intervention är den s.k. DNC-hacken från 2016, där Ryssland hade för avsikt att underminera det amerikanska presidentvalet och förbättra Donald Trumps möjligheter att vinna valet.

Då en stat bryter mot eller försummar sina skyldigheter har en folkrättsstridig handling utförts och den felande staten är därmed skyldig att ersätta den drabbade staten. Den

folkrättsstridiga handlingen bör kunna härledas till staten oavsett vilket statsorgan som utfört handlingen. Att identifiera vem som utfört ett cyberangrepp är dock problematiskt både av tekniska och juridiska skäl. Attribueringsproblematiken försvåras speciellt då stater använder sig av andra staters cyberinfrastruktur genom så kallade false-flag-operationer som kan leda till att en cyberoperation felaktigt hänförs en oskyldig stat. Detta var fallet under vinter-OS i Sydkorea år 2018, då arrangörernas datorsystem utsattes för ett storskaligt cyberangrepp innan invigningsceremonin. Nordkorea pekades snabbt ut som den ansvarige medan det i verkligheten var den ryska underrättelsetjänsten GRU som låg bakom attacken. Ryssland använde sig av nordkoreanska IP-adresser för att försöka lämna spår som skulle leda till Nordkorea. Det faktum att cyberoperationen spåras till en statlig cyberinfrastruktur är därmed inte bevis nog att staten ligger bakom cyberangreppet.

Trots att länder i allt större utsträckning har börjat publicera sina ståndpunkter, finns det fortfarande ett skriande behov för länder att offentliggöra sina ställningstaganden. I skrivande stund har Finland publicerat det färskaste ställningstagandet om folkrätten i cyberdomänen. Stater har även i allt större grad börjat offentligt anklaga andra stater för att utföra eller stöda fientliga cyberoperationer. Cyberoperationen WannaCry spårades till Nordkorea. Stater som misstänks för en sådan aktivitet har konsekvent förnekat anklagelserna eller vägrat kommentera. Enligt Nordkorea saknade dock anklagelserna laglig grund och utgjorde endast ett försök av västvärlden att ytterligare förstärka befintliga sanktioner mot landet. Det problematiska med anklagelserna är att de sällan uttrycker vilka folkrättsliga regler som har kränks eller huruvida cyberaktiviteten är förenlig med folkrätten. Cyberoperationerna beskrivs endast som t.ex. fientlig aktivitet, cybervandalism eller brott mot internationella normer. Exempelvis beskrevs WannaCry-viruset endast som brottslig användning av cyberrymden.

Sekundära skyldigheter inträder då en folkrättsstridig handling begåtts. För att en stat ska kunna vidta motåtgärder måste de vara en motreaktion på en tidigare folkrättsstridig handling som attribuerats den felande staten. Därutöver måste en skada ha skett som följd av handlingen. Å ena sidan kan stater alltid vidta åtgärder som inte bryter mot folkrätten (retorsion), t.ex. utvisa diplomater, vilket USA gjorde då 35 ryska diplomater skickades hem på grund av den ryska inbladningen i presidentvalet. Å andra sidan är motåtgärder icke-våldsamma handlingar som i sig skulle bryta mot folkrätten men är folkrättsenliga som svar på en tidigare kränkning. Den skadade staten bör alltid meddela den felande staten då motåtgärder vidtas. Syftet är att få den felande staten att upphöra med den folkrättsstridiga handlingen, återställa status quo samt gottgöra (reparation) skadan. Motåtgärderna måste vara proportionerliga till den skada som skett och den får inte utgöra en hämndaktion.

Trots bred internationell samstämmighet om folkrättens tillämpning i cyberrymden är det frågan om hur den i praktiken bör tillämpas som kvarstår som ett betydligt hinder i den normativa utvecklingen. Trots att den folkrättsliga debatten inom cyberdomänen varit framgångsrik i utvecklandet av icke-bindande vägledningar, existerar inga bindande cybertraktat och det är osäkert huruvida detta kommer att ske i framtiden. Nya sedvanerättsliga cyber normer kommer troligtvis inte utvecklas inom snar framtid, eftersom detta kräver en konsekvent och utbredd statspraxis som utvecklas med tiden.

Stater måste även agera med en rättslig övertygelse, vilket är svårt att påvisa då en stor del av staters cyberageranden inte når allmänheten, och osynlig statspraxis kan därmed inte bidra till ny sedvana. Debatten kommer troligen kvarstå som krånglig en tid framöver, och det är därmed viktigt att stater fortsätter publicera sina ståndpunkter.

BIBLIOGRAPHY

ARTICLES AND MONOGRAPHS

Antonopoulos C, *State Responsibility in Cyberspace*, in Tsagourias, N., Buchan, R. (ed), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, pp. 51-71, 2015

Aravindakshan S, *Cyberattacks: a look at evidentiary thresholds in International Law*, Indian Journal of International Law, 2020

Ayers C. E, *Rethinking Sovereignty in The Context of Cyberspace,* The United States Army War College, 2016

Banks W. C, *Symposium on Cyber Attribution: The Bumpy Road to a Meaningful International Law of Cyber Attribution*, American Journal of International Law: Vol. 113, pp. 191-196, 2019

Banks, W. C, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0,* Texas Law Review, Volume 95, Issue 7, 2017

Blank L. R, *Cyberwar/Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace*, Cyberwar: Law & Ethics for Virtual Conflicts, Oxford University Press, 2014

Boer L. J. M, *Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace*, Amsterdam Law Forum Vol. 5:3, 2013

Broeders D, van den Berg B (ed), *Governing Cyberspace: Behavior, Power, and Diplomacy*, Rowman & Littlefield, 2020

Brown G, Pollet K, *The Customary International Law of Cyberspace*, Strategic Studies Quarterly, Vol. 6, No. 3, Cyber Special Edition, Air University Press, pp. 126-145, 2012

Buchan R, Tsagourias N, *Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issue of Evidence*, Journal of Conflict and Security Law, Volume 21: Issue 3, 2016

Butterfield A, Ngondi G. E, Kerr A, *A Dictionary of Computer Science*, 7th Edition, Oxford University Press, 2016

Chircop L, *A Due Diligence Standard of Attribution in Cyberspace*, Cambridge University Press, 2018

Contreras J. L, DeNardis L, Teplinsky M, *Mapping Today's Cybersecurity Landscape*, American University Law Review, Volume 62: Issue 5, 2013

Corn G, *Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace,* 2017, in Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare (forthcoming 2018)

Corn G. P, Taylor R, *Sovereignty in the Age of Cyber*, American Society of International Law, Volume 11, pp. 207-212, 2017

Couzigou I, *Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations*, International Review of Law, Computers & Technology, 32:1, pp. 37-57, 2018

Crawford J, Olleson S, *The Character and Forms of International Responsibility,* in Malcom Evans (ed.) 'International Law' 5th Edition, Oxford University Press, 2018

Creemers R, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, in Governing Cyberspace: Behavior, Power, and Diplomacy, pp. 107-132, 2020

Crootof R, *International Cybertorts: Expanding State Accountability in Cyberspace,* 103 Cornell L. Rev. 565, 2018

Deder HG, Singer T, *Adverse Cyber Operations: Causality, Attribution, Evidence, and Due Diligence*, International Law Studies, Volume 95, pp. 430-466, 2019

Delerue F, *State Responses to Cyber Operations*, Global Relations Forum Young Academics Program, Policy Paper Series No. 5, 2017

Delerue F, *Attribution to State of Cyber Operations Conducted by Non-State Actors,* in Use and Misuse of New Technologies, pp. 233-255, Springer, 2019

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

Ducheine, P. A. L, Pijpers P. B. M. J, *The Notion of Cyber Operations,* Amsterdam Center for International Law No. 2020-08, 2020

Easterbrook F. H, *Cyberspace and the Law of the Horse*, University of Chicago Legal Forum, Chicago Unbound, 1996

Efrony D, Shany Y, *A Rulebook on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, American Journal of International Law, Volume 112, Issue 4, pp. 583-657, 2018

Egloff F. J, *Contested public attributions of cyber incidents and the role of academia*, Contemporary Security Policy, Vol. 41:1, pp. 55-81, 2020

Eichensehr K, *The Cyber-Law of Nations*, 103 Geo. L.J. 317, 2015

Eichensehr K. E, *The Law and Politics of Cyberattack Attribution*, U.C.L.A Law Review, Vol. 67, 2020

Finnemore M, Hollis D. B, *Constructing Norms for Global Cybersecurity*, The American Journal of International Law, Vol. 110, No. 3, pp. 425-479, 2016

Finnemore M, Hollis D. B, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, Temple University Legal Studies Research Paper No. 2019-14, 2019

Franzese P. W, *Sovereignty in cyberspace: can it exist?*, Air Force Law Review: Vol. 64, 2009

Geers K, *Cyberspace and the Changing Nature of Warfare*, Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, 2008

Geiss R, Lahmann H, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention*, in K. Ziolkowski (ed.) 'Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy', Tallinn, 2013

Goldsmith J, Russel S, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States In Its International Relations*, Hoover Institution Aegis Paper Series on National Security, Technology, and Law, 2018

Haataja S, *Cyber Operations and Collective Countermeasures under International Law*, Journal of Conflict and Security Law, Volume 25, Issue 1, pp. 33-51, 2020

Haataja S, *The 2007 cyber attacks against Estonia and international law on the use of force: and informational approach*, Law, Innovation and Technology, Volume 9, Issue 2, 2017

Hathaway O. A, Crootof R, Levitz P, Nix H, Nowlan A, Perdue W, Spiegel J, *The Law of Cyber-Attack,* California Law Review, Vol. 100:817, 2012

Helmersen S. T, *Finding 'the Most Highly Qualified Publicists': Lessons from the International Court of Justice*, European Journal of International Law, Volume 30, Issue 2, pp. 509-535, 2019

Henriksen A, *Lawful State Responses to Low-Level Cyber-Attacks*, Nordic Journal of International Law, Volume 84:Issue 2, 2015

Henriksen A, *The end of the road for the UN GGE process: The future regulation of cyberspace*, Journal of Cybersecurity: Vol. 5, No.1, 2019

Hollis D. B, *An e-SOS for Cyberspace*, Harvard International Law Journal, Volume 52, Issue 2, 2011

Hollis D. B, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?* Cyberwar: Law & Ethics for Virtual Conflicts, Oxford University Press, 2014

Huang Z, Macak K, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, Chinese Journal of International Law, Volume 16, Issue 2, pp. 271-310, 2017

Isbell R, Duffy A, Norris P, Watson T, Nicholson A, *A Taxonomy of Technical Attribution Techniques for Cyber Attacks*, 11th European Conference on Information Warfare and Security, ECIW 2012, pp. 188-197, 2012

Jensen E. T, *State Obligations in Cyberspace*, 14 Baltic Yearbook of International Law 71, 2014

Jensen E. T, *The Tallinn Manual 2.0: Highlights and Insights*, 48 Georgetown Journal of International Law 735, 2017

Jensen E. T, Watts S, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?* 95 Texas Law Review 1555, 2017

Jiang Z, *Regulating the Use and Conduct of Cyber Operations Through International Law: Challenges and Fact-Finding Body Proposal*, LSE Law Review, 2019

Johnson D. R, Post, D. G., *Law and Borders – the Rise of Law in Cyberspace*, Stanford Law Review, Vol. 48, 1996

Kamal A, *The Law of Cyber-space: An Invitation to The Table of Negotiations*, Geneva, United Nations Institute for Training and Research, Palais des Nations, 2005

Kanuck S, *Sovereign Discourse on Cyber Conflict under International Law*, Texas Law Review, Vol. 88:1571, pp. 1571-1597, 2010

Kittichaisaree K, *Public International Law of Cyberspace*, Springer, 2017

Koh H. H, *The Trump Administration and International Law*, Washburn Law Journal, pp. 413-469, 2017

Kosseff J, *Retorsion as a Response to Ongoing Malign Cyber Operations*, NATO CCDCOE Publications, Tallinn, 2020

Kueh D. T, *From Cyberspace to Cyberpower: Defining the Problem*, in Cyberpower and National Security, University of Nebraska Press, 2009

Kurbalija J, *State Responsibility in Digital Space*, Swiss Review of International & European Law, Issue 2, 2016

Leiter A, *Cyber Sovereignty: A Snapshot From A Field In Motion*, Harvard International Law Journal Frontiers, Volume 61/2020, 2020

Liaropoulos A, *Power and Security in Cyberspace: Implications for the Westphalian State System*, 2011

Liaropoulos A, *War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory*, 2010

Lin H, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, Hoover Institution Aegis Paper Series on National Security, Technology, and Law, 2016

Macak K, *On the Shelf, but Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law*, 113 AJIL Unbound 81, 2019

Mauer T, *'Proxies' and Cyberspace*, Journal of Conflict & Security Law, Vol. 21 No. 3, pp. 383-403, 2016

Moynihan H, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, Chatham House Research Paper, 2019

Mueller M. L, *Against Sovereignty in Cyberspace*, International Studies Review, 2019

Nolte G, *From Dionisio Anzilotti to Roberto Ago: The Classical International Law of State Responsibility and the Traditional Primacy of a Bilateral Conception of Inter-state Relations,* European Journal of International Law, Vol. 13, No. 5; pp. 1083-1098, 2002

Payne C, Finlay L, *Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack*, 49 Geo Wash Int'l Rev 535, 2017

Payne T, *Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations*, Lewis & Clark Law Review, Vol. 20:2, pp. 683-715, 2016

Pihelgas M, *Back-Tracing and Anonymity in Cyberspace*, in Ziolkowski K (ed.), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, Tallinn, 2013

Pirker B, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in Ziolkowski K (ed.), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, Tallinn, 2013

Provost R (ed), *State Responsibility in International Law*, Routledge, 2002

Rid T, Buchanan B, *Attributing Cyber Attacks*, Journal of Strategic Studies, Vol. 38, Nos. 1-2, 4-37, 2015

Roguski P, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program For Cyber Norms Policy Brief, 2020

Roguski P, *Violations of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach*, in 'Governing Cyberspace: Behavior, Power, and Diplomacy, 2020

Romanosky S, Goldman Z, *Understanding Cyber Collateral Damage*, Journal of National Security Law & Policy, Vol. 9:233, 2017

Ronen Y, *Some Evidentiary Dimensions of Attributing Unlawful Cyber Operations to States*, Hebrew University of Jerusalem Legal Research Paper 20-11, 2020

Roscini M, *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*, Max Planck Yearbook of United Nations Law, Volume 14, p. 85-130, 2010

Ruys T, *Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework*, Research Handbook on UN Sanctions and International Law, Edward Elgar Publishing, 2016

Sander B, *Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections,* Chinese Journal of International Law, Volume 18, Issue 1, pp. 1-56, 2019

Sander B, *The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations*, NATO CCD COE Publications, Tallinn, 2019

Schmitt M. N, *Cyberspace and International Law: The Penumbral Mist of Uncertainty,* 126 Harv. L. Rev. F. 176, 2013

Schmitt M. N (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013

Schmitt M. N, *"Below the Threshold" Cyber Operations*, Virginia Journal of International Law, Vol. 54, 2014

Schmitt M. N, *The Law of Cyber Warfare: Quo Vadis?*, Stanford Law & Policy Review, Vol. 25:269, 2014

Schmitt M. N, Vihul L, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, Fletcher Security Review, Vol. 1, Issue II, 2014

Schmitt M. N, Vihul L, *The Nature of International Law Cyber Norms,* Tallinn Papers No. 5, NATO Cooperative Cyber Defence of Excellence, 2014

Schmitt M. N, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretative and Applicative Precision*, Israel Law Review, 48, pp. 81-109, 2015

Schmitt M. N, *Grey Zones in the International Law of Cyberspace*, 42:2 Yale Journal of International Law Online, 2017

Schmitt M. N, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 Harvard National Security Journal 239, 2017

Schmitt M. N, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017

Schmitt M. N, Vihul L, *Respect for Sovereignty in Cyberspace*, Texas Law Review, Volume 95, Issue 7, 2017

Schmitt M. N, Vihul, L, *Sovereignty In Cyberspace: Lex Lata Vel Non,* American Society of International Law, Volume 111, pp. 213-218, 2017

Schmitt M. N, *Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, Chicago Journal of International Law: Vol. 19: No. 1, Article 2, 2018

Schmitt M. N, *Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace*, Texas National Security Review: Volume 3, Issue 3, pp. 33-47, 2020

Shackelford S. J, *Governing New Frontiers in the Information Age: Toward Cyber Peace*, Cambridge University Press, 2020

Shackelford S. J, *State Responsibility for Cyber Attacks: Competing Standards For a Growing Problems*, CCD CCOE Publications, Tallinn, pp. 197- 208, 2010

Shany Y, Schmitt M. N, *An International Attribution Mechanism for Hostile Cyber Operations*, International Law Studies, Volume 96, pp. 196-222, 2020

Spector P, *In Defense of Sovereignty, in the Wake of Tallinn 2.0*, American Society of International Law, Volume 111, pp. 219-223, 2017

Sullivan C, *The 2014 Sony Hack and The Role of International Law*, Journal of National Security, Law & Policy, Vol. 8, No. 3, 2014

Teplinsky M, *Fiddling on the Roof: Recent Developments in Cybersecurity*, American University Business Law Review, Vol. 2, No. 2, 225, 2013

Tikk E, *International Law in Cyberspace: Mind the Gap*, Cyber Policy Institute, 2020

Trautman J. L, Ormerod, P. C., *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things,* University of Miami Law Review, Vol. 72:761, 2018

Tsagourias N, *Cyber Attacks, Self-Defence and the Problem of Attribution*, Journal of Conflict & Security Law, Vol. 17 No. 2, pp. 229-244, 2012

Tsagourias N, *The Law Applicable to Countermeasures Against Low-Intensity Cyber Operations*, Baltic Yearbook of International Law, Volume 14, 2014

Tsagourias N, *The legal status of cyberspace*, Research Handbook on International Law and Cyberspace, pp. 13-29, Edward Elgar Publishing, 2015

Tsagourias N, *Law, Borders and the Territorialisation of Cyberspace*, Indonesian Journal of International Law, 2018

Tsagourias N, Farell M, *Cyber Attribution: Technical and Legal Approaches and Challenges*, European Journal of International Law, 2020

Väljataga A, *Tracing opinio juris in National Cyber Security Strategy Documents,* NATO CCDCOE, Tallinn, 2018

Walton B, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 Yale Law Journal, Issue 5, 2017

Watts S, *Low-Intensity Cyber Operations and the Principle of Non-intervention*, in Cyber War: Law and Ethics for Virtual Conflicts, 2015

Yeli H, *A Three-Perspective Theory of Cyber Sovereignty*, PRISM Volume 7, No. 2, 2017

Ziolkowski K (ed.), *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*, NATO CCDCOE, Tallinn, 2013

Ziolkowski K, *Stuxnet – Legal Considerations,* NATO CCDCOE, Tallinn, 2012

CONVENTIONS AND TREATIES

1945 The Charter of the United Nations

1945 Statute of the International Court of Justice, 26 June 1945, 59. Stat. 1055, 33 UNTS 993

1949 The North Atlantic Treaty

1969 Vienna Convention on the Law of Treaties, 23 May 1969

1970 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States

2001 Convention on Cybercrime (Budapest Convention on Cybercrime) Council of Europe

INTERNATIONAL JURISPRUDENCE

INTERNATIONAL COURT OF JUSTICE

North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands); International Court of Justice (ICJ), 20 February 1969.

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, ICJ Reports 1971

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); International Court of Justice (ICJ), 27 June 1986.

Case Concerning United States Diplomatic and Consular Staff in Tehran (United States v. Iran) 29 November 1980

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia), International Court of Justice (ICJ), 11 July 1996

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports, 8 July 1996

Gabčikovo–Nagymaros Project (Hungary v. Slovakia), Judgment, I.C.J. Reports, 25 September 1997.

Oil Platforms (Islamic Republic of Iran v. United States of America), ICJ Reports, 2003, 161 Separate Opinion on Judge Simma

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Judgment, ICJ Reports, 16 December 2015

PERMANENT COURT OF INTERNATIONAL JUSTICE

Case of the S.S. "Wimbledon" (United Kingdom, France, Italy & Japan v. Germany), 1923

Settlers of German Origin in Poland, Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 6 (Sept. 10)

S.S. Lotus (France v. Turkey), 1927, P.C.I.J (ser. A) No. 10 (Sept. 7)

Island of Palmas (Netherlands v. US) 2 R.I.A.A 829, 838 (Perm. Ct. Arb. 1928).

Factory at Chorzów (Germany v. Poland), 13 September 1928 (ser. A) No. 17

Phosphates in Morocco (Italy v. France), 1938 P.C.I.J (ser. A/B) No. 74 (June 14)

ABRTIAL TRIBUNAL

Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two states and which related to the problems arising from the Rainbow Warrior Affair, 30 April 1990, 20 RIAA 217.

UN DOCUMENTS

DECLARATIONS

Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, UNGA Res 2626 (XXV) (24 October 1970).

RESOLUTIONS

The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission, 53rd session, (Apr. 23-June 1,July 2-Aug. 10, 2001), General Assembly Official Records, 56th session, supp. no. 10, UN Doc. A/56/10.

Resolution adopted by the General Assembly, Responsibility of States for internationally wrongful acts, A/RES/56/83 28 January 2002

Resolution adopted by the General Assembly on 2 December 2004, Responsibility of States for internationally wrongful acts, A/RES/59/35 16 December 2004

Developments in the field of information and telecommunications in the context of international security (A/RES/58/32) 18 December 2003

Developments in the field of information and telecommunications in the context of international security (A/RES/60/45) 6 January 2006

Developments in the field of information and telecommunications in the context of international security (A/RES/66/24) 13 December 2011

Developments in the field of information and telecommunications in the context of international security (A/RES/68/243) 9 January 2014

Developments in the field of information and telecommunications in the context of international security (A/RES/70/237) 30 December 2015

Developments in the field of information and telecommunications in the context of international security (A/RES/73/27) 11 December 2018

Advancing responsible State behavior in cyberspace in the context of international security (A/RES/73/266) 2 January 2019

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security:

Report of the Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security (A/65/201) 30 July 2010

Report of the Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security (A/68/98) 24 June 2013

Report of the Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security (A/70/174) 22 July 2015

UN Open-ended Working Group

Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

International Law Commission

Second report on the identification of customary international law, (UN/A/CN.4/672), 22 May 2014

Identification of Customary International Law, Text to the draft conclusion as adopted by the Drafting Committee on second reading, UN/A/CN.4/L.908, 17 May 2018, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/136/30/PDF/G1813630.pdf?OpenElement

EUROPEAN UNION

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, June 7, 2017)

Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 20 November 2017

Joint Statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian Cyber Attacks' 4 October 2018, https://www.consilium.europa.eu/sv/press/press-releases/2018/10/04/joint-statement-by-presidents-tusk-and-juncker-and-high-representative-mogherini/.

Council Decision (CFSP) 2019/797 of 17 May 2019, Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or its Member States, 2019 O.J. (L 129) 13 (EC)

Council of the European Union, 'Declaration by the High Representative on behalf of the European Union – call to promote and conduct responsible behaviour in cyberspace', 21 February 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/.

European Council, Press release, EU imposes the first ever sanctions against cyber-attacks, 30 July 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE

Permanent Council Decision No. 1202, OSCE Confidence-Building Measures To Reduce The Risks of Conflict Stemming From The Use of Information And Communication Technologies, 10 March 2016, PC.DEC/1202

NORTH ATLANTIC TREATY ORGANIZATION

Wales Summit Declaration (Issued by the Head of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014,

NATIONAL DOCUMENTS

Australia

Australia's International Cyber Engagement Strategy, *Australia's position on how international law applies to state conduct in cyberspace*,

https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html

Austria

Pre-Draft Report of the OEWG – ICT, Comments by Austria, 31 March 2020, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf

China

International Strategy of Cooperation on Cyberspace Contents' (2017), unofficial English translation http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

Czech Republic

Statement by Mr. Richard Kadlcak, Special Envoy for Cyberspace, 2nd substantive session on the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, 11 February 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

Estonia

Declaration of the Minister of Foreign Affairs of the Republic of Estonia, 1 May 2007, https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia.

President of Estonia, *International Law Applies also in Cyber Space*, 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html

Finland

Ministry For Foreign Affairs, *International law and cyberspace – Finland's national positions*, 15 October 2020, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

France

Ministère des Armées, *Droit International Appliqué Aux Opérations Dans Le Cyberspace*, 9 September 2019, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf; English translation https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

Ministry for Europe and Foreign Affairs, 'Paris Call for Trust and Security in Cyberspace', 12 November 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Germany

Deutscher Bundestag, *Militärische, völkerrechtliche und rüstungskontrollpolitische Aspekte der Cyber-Sicherheit* 17 May 2011, https://www.bundestag.de/resource/blob/413608/f7d0a223f832f8a63b52f32308ae2eea/WD-2-099-11-pdf-data.pdf

Deutscher Bundestag, *Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare),* 24 February 2015, https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbee41d8d3d6898/WD-2-038-15-pdf-data.pdf

Iran

General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat, 18 August 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat

Russia

Convention on International Information Security, 22 September 2011, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Press statements following Russian-Chinese talks, 25 June 2016, http://en.kremlin.ru/events/president/transcripts/52273.

Joint Statement Between The Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

Russian Federation, *Doctrine of Information Security of the Russian Federation*, 5 December 2017, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

The Netherlands

Ministry of Defence, *Defence Cyber Strategy*, 2015, https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy

Ministry of Defence, *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW*, 4 October 2018, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

Ministry of General Affairs, *Joint statement by Prime Minister May and Prime Minister Rutte on cyber activities of the Russian military intelligence service, the GRU,* 4 October 2018, https://www.government.nl/latest/news/2018/10/04/joint-statement-by-prime-minister-may-and-prime-minister-rutte-on-cyber-activities-of-the-russian-military-intelligence-service-the-gru

Government of the Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', 4 October 2018, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 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

The United States

US Department of Defense, Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations', May 1999, https://fas.org/irp/eprint/io-legal.pdf.

The United States Army, *Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010, https://fas.org/irp/doddir/army/pam525-7-8.pdf

The White House, *International Strategy for Cyberspace*, May 2011 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Legal Advisor U.S Department of State, Harold Hongju Koh, *International Law in Cyberspace*, 18 September 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm

US Department of State, Digest of United States Practice in International Law (2014) https://2009-2017.state.gov/documents/organization/244486.pdf.

US Homeland Security, 'Statement By Secretary Johnson on Cyber Attack On Sony Pictures Entertainment', December 19, 2014. https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment

The US Department of Defense, 'The Department of Defense Cyber Strategy' (2015) https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

The White House, Office of the Press Secretary, *Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea"*, 2 January 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s

The White House, Office of the Press Secretary, *Statement by the President on Progress in the Fight Against ISIL*, 13 April 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/04/13/statement-president-progress-fight-against-isil

U.S. Department of State, Legal Adviser Brian J. Egan, *Remarks on International Law and Stability in Cyberspace* (2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

The White House, Thomas P. Bossert, 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea', December 19, 2017 https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Joint Publication 3-12, *Cyberspace Operations*, 8 June 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Office of the Director of National Intelligence, 'A Guide to Cyber Attribution', 14 September 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf .

United States, Department of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations,* 4 October 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

U.S. Department of State, *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, 23 September 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

The US Department of State, Statement by the Secretary of State Michael R. Pompeo, *The United States Condemns Russian Cyber Attack Against the Country of Georgia*, 20 February 2020, https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

U.S. Department of Defence, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference', 2 March 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

The United Kingdom

Foreign & Commonwealth Office, Foreign Secretary Philip Hammond, *Foreign Secretary responds to FBI reports into cyber attacks on Sony Pictures*, Press Release 19 December 2014, https://perma.cc/46BN-RG5P

United Kingdom, *National Cyber Security Strategy 2016-2021*, HM Government, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Statement of Foreign Office Minister, Lord Ahmad, *Foreign Office Minister condemns North Korean actor for WannaCry attacks*, 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

Department of Health, National Audit Office, Report by the Comptroller and Auditor General, *Investigation: WannaCry cyber attack and the NHS*, HC 414, Session 2017-2019, 25 April 2018, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Speech by Attorney General Jeremy Wright, *Cyber and International Law in the 21st Century*, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

National Cyber Security Centre, Annual Review 2019, https://www.ncsc.gov.uk/news/annual-review-2019

Foreign & Commonwealth Office, *UK condemns Russia's GRU over Georgia cyber-attacks*, 20 February 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

National Cyber Security Centre, *Advisory: APT29 targets COVID-19 vaccine development*, 16 July 2020, https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

INTERNET SOURCES

NB: All the Internet sources have been accessed last on 1 November 2020.

Adrian Venables, *Establishing Cyber Sovereignty – Russia Follows China's Example*, 20 March 2019, https://icds.ee/establishing-cyber-sovereignty-russia-follows-chinas-example/.

Adrijana Gavrilovic, *[Web discussion summary] Applicability of international law to cyberspace: Do we know the rules of the road?*, 12 November 2019, https://www.diplomacy.edu/blog/web-discussion-summary-applicability-international-law-cyberspace-do-we-know-rules-road.

Alex Grisby, *The Year in Review: The Death of the UN GGE Process?*, 21 December 2017, https://www.cfr.org/blog/year-review-death-un-gge-process.

Andreas Zimmerman, *International Law and 'Cyber Space'* (2014), available at https://esil-sedi.eu/wp-content/uploads/2014/01/ESIL-Reflections-Andreas-Zimmermann_0.pdf.

Andy Greenberg, *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History*, 17 October 2019, Wired, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

Anushka Kaushik, *Public attribution and its scope and efficacy as a policy tool in cyberspace* (2019), https://www.orfonline.org/expert-speak/public-attribution-and-its-scope-and-efficacy-as-a-policy-tool-in-cyberspace-56826/.

Ashley Deeks, *Defend Forward and Cyber Countermeasures*, 12 August 2020, Lawfare, https://www.lawfareblog.com/defend-forward-and-cyber-countermeasures.

Axel Scroxton, *EU sanctions China and Russia over cyber attacks*, 31 July 2020, Computer Weekly, https://www.computerweekly.com/news/252486952/EU-sanctions-China-and-Russia-over-cyber-attacks.

Bardo Fassbender, *Westphalia, Peace of (1648)*, Max Planck Encyclopedias of International Law, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e739.

BBC News, David Lee, *Israel tops cyber-readiness poll but China lags behind*, 8 March 2012, https://www.bbc.com/news/technology-16787509

BBC News, *Estonia fines man for 'cyber war*, 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.

BBC News, *Georgia hit my massive cyber-attack*, 28 October 2019, https://www.bbc.com/news/technology-50207192.

BBC News, Joe Tidy, *Police launch homicide inquiry after German hospital hack*, 18 September 2020, https://www.bbc.com/news/technology-54204356

BBC News, Jonathan Fildes, *Stuxnet virus targets and spreads revealed*, 15 February 2011, https://www.bbc.com/news/technology-12465688.

BBC News, *Nato: Cyber-attack on one nation is attack on all*, 27 August 2019, https://www.bbc.com/news/technology-49488614.

BBC News, *NHS cyber-attack: GPs and hospitals hit by ransomware*, 13 May 2017, https://www.bbc.com/news/health-39899646

BBC News, *NHS cyber-attack: No 'second spike' but disruption continues*, 15 May 2017, https://www.bbc.com/news/uk-39918426.

BBC News, *North Korea calls UK WannaCry accusations 'wicked'*, 31 October 2017, https://www.bbc.com/news/world-asia-41816958.

BBC News, *Ransomware cyber-attack: Who has been hardest hit?,* 15 May 2017, https://www.bbc.com/news/world-39919249.

BBC News, *Russia cyber-plots: US, UK and Netherlands allege hacking*, 4 October 2018, https://www.bbc.com/news/world-europe-45746837.

BBC News, *UK and US blame Russia for 'malicious' NotPetya cyber-attack*, 15 February 2018, https://www.bbc.com/news/uk-politics-43062113

BBC News, *US 'launched cyber-attack on Iran weapons systems'*, 23 June 2019 https://www.bbc.com/news/world-us-canada-48735097.

BBC News, *Why did North Korea's internet go down?*, 23 December 2014, https://www.bbc.com/news/world-asia-30586940

BBC News, *Winter Olympics hit by cyber-attack*, 12 February 2018, https://www.bbc.com/news/technology-43030673.

Bruce Schneier, *Did North Korea Really Attack Sony?,* 22 December 2014, The Atlantic, https://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/

CCDCOE, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/

CCDCOE, Katriina Härmä, Tomas Minarik, *European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox,* https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/

CCDCOE, *Over 50 States Consult Tallinn Manual 2.0*, 2 February 2016, https://ccdcoe.org/news/2016/over-50-states-consult-tallinn-manual-2-0/
CCDCOE, *Trends In International Law For Cyberspace*, May 2019, https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf

CCDCOE, *WannaCry Campaign: Potential State Involvement Could Have Serious Consequences* (2017), https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/.

Christopher Woody, *NATO leaders are worried about cyberattacks, but it's not clear they all agree on what that means*, 2 October 2018, Business Insider, https://www.businessinsider.com/nato-leaders-agree-cyberattacks-are-threat-but-cant-agree-definition-2018-10?r=US&IR=T.

Colonel Gary Corn, Just Security, Tallinn Manual 2.0 – Advancing the Conversation, February 15, 2017 https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/

Corfield, G., *WannaCry ransomware attack on NHS could have triggered NATO reaction, says German cybergeneral*, The Register, 3 February 2020, https://www.theregister.com/2020/02/03/wannacry_nato_response/

CRF, https://www.cfr.org/cyber-operations/notpetya.

CSIS Report on Significant Cyber Incidents, Center for Strategic and International Studies (CSIS) Report, https://www.csis.org

CyberPeace Alliance, *Tallinn Manual – A Brief Review of the International Law Applicable to Cyber Operations*, 6 December 2019, https://medium.com/@cyberpeacealliance/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2

Cybersecurity and Infrastructure Security Agency (CISA), 'COVID-19 Exploited by Malicious Cyber Actors', 8 April 2020, https://www.us-cert.gov/ncas/alerts/aa20-099a.
Dagmar Richter, *Unfriendly Act*, Max Planck Encyclopedia of Public International Law [MPEPIL], https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e423;

Dan Roberts, *Obama imposes new sanctions against North Korea in response to Sony hack*, 2 January 2015, The Guardian, https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.

Daniel Stauffacher, *Prospects and Challenges of Developing International Cybersecurity Norms in the UN,* 29 May 2019, available at https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf.

Data Protection, *WannaCry Ransomware Attack Summary*, 17 May 2017, https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/.

David E. Sanger, Nick Corosaniti, *D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump*, 14 June 2016, The New York Times, https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

David E. Sanger, *Obama Ordered Sped Up Wave of Cyberattacks Against Iran,* 1 June 2012, The New York Times, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html;

Declaration by Miguel Rodríguez, Representative of Cuba, At the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 23 June 2017, https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

Dennis Broeders, Fabio Cristiano, *Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road*, 2 April 2020, https://www.ispionline.it/it/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417.

Duncan B. Hollis, *Could Deploying Stuxnet be a War Crime?*, 25 January 2011, Opinio Juris, http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/.

Duncan B. Hollis, *Could Deploying Stuxnet be a War Crime?*, 25 January 2011, Opinio Juris, http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/.

Duncan B. Hollis, *Four Challenges for International Law and Cyberspace: Sartre, Baby Carriages, Horses, and Simon& Garfunkel Part 2*, 7 May 2019, Council on Foreign Relations, https://www.cfr.org/blog/four-challenges-international-law-and-cyberspace-sartre-baby-carriages-horses-and-simon-0.

Duncan B. Hollis, *Improving Law and State Cyber Operations: Fourth Report*, 5 March 2020, http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1.pdf

Duncan B. Hollis, *Improving Law and State Cyber Operations: Improving Transparency,* 9 August 2018, http://www.oas.org/en/sla/iajc/docs/CJI_doc_570-18.pdf

E-Estonia, *e-governance*, https://e-estonia.com/solutions/e-governance/i-voting/

Duncan B. Hollis, *Elaborating International Law for Cyberspace*, 29 July 2020, https://directionsblog.eu/elaborating-international-law-for-cyberspace/.

Ellen Nakashima, Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say*, 2 June 2012, The Washington Post, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html;

Ellen Nakashima, *Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say,* 25 February 2018, the Washington Post, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

Ellen Nakashima, *U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election,* 25 December 2019, The Washington Post, https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

Emilie Legris, Dimitri Walas, *ESIL Reflection: Regulation of Cyberspace by International Law* (2018), https://esil-sedi.eu/fr/esil-reflection-regulation-of-cyberspace-by-international-law/.

Emmanuelle Walkowiak, *Russia's meddling in the French elections: How and why?*, 24 May 2017, available at https://electionwatch.unimelb.edu.au/articles/russias-meddling-in-the-french-elections-how-and-why.

ESIL Reflection Cyber Insecurity and the Politics of International Law https://esil-sedi.eu/post_name-1148/

European Union Agency for Cybersecurity (ENISA), Glossary, 'Ransomware', https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware.

Francesca Casali, Stefania Di Stefano, *State behaviour in cyberspace: a new challenge for the international community*, 13 March 2018, https://www.diplomacy.edu/blog/state-behaviour-cyberspace-new-challenge-international-community.

François Delerue, Elaine Korzak, *From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity*, 27 January 2020, Council on Foreign Relations, https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity.

François Delerue, *International Law In Cyberspace Matters: This Is How And Why*, May 2019, https://eucyberdirect.eu/wp-content/uploads/2019/05/francois-delerue-international-law-in-cyberspace-matters-may-2019-eucyberdirect.pdf

Gareth Corfield, *WannaCry ransomware attack on NHS could have triggered NATO reaction, says German cybergeneral*, The Register, 3 February 2020, https://www.theregister.com/2020/02/03/wannacry_nato_response/.

Gary Corn, *Tallinn Manual 2.0 – Advancing the Conversation*, Just Security, 15 February 2017, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/

Gerard O'Dwyer, *Finland's security agencies collaborate after cyber attacks*, 29 August 2019, https://www.computerweekly.com/news/252469691/Finlands-security-agencies-collaborate-after-cyber-attacks.

Giorgi Nakashidze, *Cyberattack against Georgia and International Response: emerging normative paradigm of 'responsible state behavior in cyberspace'?,* 28 February 2020, https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/.

GIP Digital Watch Observatory https://dig.watch/processes/un-gge

Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, November 2019, https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

Greenberg, A., *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History*, Wired, 17 October 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

Greg Miller, Ellen Nakashima, Adam Entous, *Obama's secret struggle to punish Russia for Putin's election assault*, 23 June 2017, The Washington Post, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.d5ada09b5d4f.

Hal Brands, *Paradoxes of the Gray Zone*, 5 February 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.
Harriet Moynihan, *Power Politics Could Impede Progress on Responsible Regulation of Cyberspace*, 3 December 2019, https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace?gclid=EAIaIQobChMIrYfMtq7C6QIVhqsYCh3aXAecEAAYASAAEgLqYfD_BwE

Healey, J., *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council, 2012 https://www.atlanticcouncil.org/wpcontent/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF

Ian Traynor, *Web attackers used a million computers, says Estonia*, 18 May 2007, The Guardian, https://www.theguardian.com/technology/2007/may/18/news.russia.

ILC, *Analytical Guide to the Work of the International Law Commission*, https://legal.un.org/ilc/guide/9_6.shtml.

International and Foreign Cyberspace Law Research Guide, Georgetown Law, https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478
Internet World Stats, https://www.internetworldstats.com/emarketing.htm

Jack Stubbs, Exclusive: *Wannacry hits Russian postal service, exposes wider security shortcomings*, 24 May 2017, Reuters, https://www.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUSKBN18K26O.

Jack Stubbs, Joseph Menn, Christopher Bing, *Inside the West's failed fight against China's 'Cloud Hopper' hackers*, Reuters, 26 June 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

Jacob Morgan, *A Simple Explanation of 'The Internet Of Things'* 13 May 2014, Forbes, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7ca2a4f01d09.

James Crawford, State Responsibility, Max Planck Encyclopedia of Public International Law [MPEPIL], September 2006, Oxford Public International Law, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1093?prd=EPIL

James Crawford, *The International Law Commission's Articles on State Responsibility: Past and Future*, UN Audiovisual Library, https://legal.un.org/avl/ls/Crawford_S.html.

James Rothwell, *Iran accused of attempting cyberattack on World Health Organisation*, the Telegraph, 2 April 2020, https://www.telegraph.co.uk/news/2020/04/02/iran-accused-attempting-cyber-attack-world-health-organisation/

Jeffrey Biller, Michael Schmitt, *Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences* 24 October 2018, EJIL:Talk! https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/.

Joan E. Greve, *Steady drumbeat of misinformation*, The Guardian, 17 September 2020, https://www.theguardian.com/us-news/2020/sep/17/misinformation-us-elections-2020-russia

Joseph Marks, *The Cybersecurity 202: The Sony hack ushered in a dangerous era in cyberspace*, 27 November 2019, The Washington Post, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/27/the-cybersecurity-202-the-sony-hack-ushered-in-a-dangerous-era-in-cyberspace/5ddd716c602ff1181f264147/.

Julian E. Barnes, The New York Times, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, 28 August 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html?action=click&module=Top%20Stories&pgtype=Homepage

Justin Sherman, 'How Much Cyber Sovereignty is Too Much Cyber Sovereignty?', 30 October 2017, Council on Foreign Relations, https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

Katja S Siegler, *Domaine Reservé* MEPIL, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398.

Keiko Kono, *International Laws on Cyber attacks that Do Not Constitute an Armed Attack*, http://www.nids.mod.go.jp/english/publication/briefing/pdf/2017/briefing_e201710.pdf 2017

Kersti Kaljulaid, President of the Republic Opening Speech at CyCon 2017, 31 May 2017, https://www.president.ee/en/official-duties/speeches/13324-president-of-the-republic-opening-speech-at-cycon-2017-31-may-2017/index.html

Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History (*2011), available at https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid* 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Kubo Macak, Tilman Rodenhäuser, Laurent Gisel, *Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?,* 2 April 2020, https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/.

Larry D. Welch, *Cyberspace – The Fifth Operational Domain*, 2011, https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf

Leandros Maglaras, Mohammed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, Helge Janicke, Stylianos Rallis, 'Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures' (2019), https://arxiv.org/pdf/1901.03899.pdf.

Liviu Arsene, *5 Times More Coronavirus-themed Malware Reports during March*, 20 March 2020, https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/.

Marc Schack, *Did the US Stay "Well Below the Threshold of War" With its June Cyberattack on Iran?,* EJIL: Talk!, 2 September 2019, http://www.ejiltalk.org/did-the-us-stay-well-below-the-threshold-of-war-with-its-june-cyberattack-on-iran/

Mark Pomerleau, *What is 'sovereignty' in cyberspace? Depends who you ask*, 21 November 2019, https://www.fifthdomain.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/.

Matthew Field, *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled*, 11 October 2018, The Daily Telegraph, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

McAfee, *What Is Stuxnet?* https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.

Michael J. Adams, *A Warning About Tallinn 2.0… Whatever It Says,* Lawfare, 4 January 2017, https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says

Michael J. Adams, Megan Reiss, *How Should International Law Treat Cyberattacks like WannaCry?,* 22 December 2017, Lawfare, https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry.

Michael Schmitt, *Cyber Responses "By The Numbers" in International Law*, 4 August 2015, EJIL: Talk!, https://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/

Michael Schmitt, *Estonia Speaks Out on Key Rules for Cyberspace*, 10 June 2019, Just Security https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.

Michael Schmitt, *In Defense of Sovereignty in Cyberspace*, 8 May 2018, Just Security, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

Michael Schmitt, Jeffrey Biller, *The NotPetya Cyber Operation as a Case Study of International Law*, 11 July 2017, EJIL: Talk! https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/-

Michael Schmitt, Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, 30 June 2017, Just Security, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Michael Schmitt, Sean Fahey, *WannaCry and the International Law of Cyberspace,* 22 December 2017, Just Security, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/.

Michael Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, Just Security, 9 February 2017, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis,* 14 October 2019, Just Security, https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.

Michele Markoff, U.S. Expert to the GGE, *Explanation of Position at the Conclusion of the 2016-201 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/.

Microsoft, *A Digital Geneva Convention to protect cyberspace*, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

Mike Levine, *Russia tops list of 100 countries that could launch cyberattacks on US*, 18 May 2017, ABC News, https://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188.

Miller, G., Nakashima, E., Entous, A., *Obama's secret struggle to punish Russia for Putin's election assault*, The Washington Post, 23 July 2017, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.d5ada09b5d4f

Murcia Today, *Cyber-attack threatens Spanish hospital computer systems*, 24 March 2020, https://murciatoday.com/cyber_attack_threatens_spanish_hospital_computer_systems_1367723-a.html.

Nakashima, E., *Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say*, The Washington Post, 25 February 2018, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-

olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

NATO CCDCOE, 11th International Conference on Cyber Conflict (CyCon 2019), Michael Schmitt *Sovereignty and Cyber Operations*, https://www.youtube.com/watch?v=u0Ikg8RjITY&t=1241s.

NATO CCDCOE, 4th annual International Conference on Cyber Conflict (CyCon), *CyCon 2012, Michael Schmitt: Tallinn Manual part 1*, https://www.youtube.com/watch?v=wY3uEo-Itso.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *WannaCry Campaign: Potential State Involvement Could Have Serious Consequences*, 2017, https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/.

NATO Glossary of Terms and Definitions (AAP-07, Edition 2019), https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF.

Nicholas Thompson, 'UN Secretary-General: US-China Tech Divide Could Cause More Havoc Than the Cold War', 15 January 2020, https://www.wired.com/story/un-secretary-general-antonio-guterres-internet-risks/.

Nick Allen, *Dutch spies 'caught Russian election hackers on camera*, 26 January 2018, https://www.telegraph.co.uk/news/2018/01/26/dutch-spies-caught-russian-election-hackers-camera/.

The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

Paolo Passeri, *2015 Cyber Attacks Statistics*, HACKMAGEDDON, 11 January 2016, https://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/.

Paolo Passeri, *Q1 2020 Cyber Attacks Statistics*, HACKMAGEDDON, 14 April 2020, https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/.

Piret Pernik, *Responding to "the Most Destructive and Costly Cyberattack in History"*, 23 February 2018, https://icds.ee/responding-to-the-most-destructive-and-costly-cyberattack-in-history/.

President Toomas Hendrik Ilves' keynote speech at the 3rd Annual Billington Cybersecurity Summit, Washington DC, 27 September 2012, https://vp2006-2016.president.ee/en/official-duties/speeches/8003-president-toomas-hendrik-ilves-keynote-speech-at-the-3rd-annual-billington-cybersecurity-summit-washington-dc-september-27th-2012/index.html

Przemyslaw Roguski, *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations Part I'*, 24 September 2019, Opinio Juris,

http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.

Przemyslaw Roguski, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, 6 March 2020, Just Security, https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Przemyslaw Roguski, *The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States*, 11 May 2020, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/

Radoslaw Fordonski, Wojciech Kasprzak, *WannCry ransomware cyberattack as violation of international law*, pp. 47-73, https://wpia.uwm.edu.pl/czasopisma/sites/default/files/uploads/Studia_Prawno_Ustrojowe/2019/44/47-73.pdf

Reuters, *Cyber attack hits 200,000 in at least 150 countries: Europol*, 14 May 2017, https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX

Richter, D., *Unfriendly Act*, Max Planck Encyclopedia of Public International Law [MPEPIL], https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e423, 2013

Russel Goldman, *What We Know and Don't Know About the International Cyberattack*, 12 May 2017, New York Times, https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html.

Salem Alelyani, Harnish Kumar G. R., *Overview of Cyberattack on Saudi Organizations* (2018). https://journals.nauss.edu.sa/index.php/JISCR/article/download/455/464/0

Scarlet Kim, Paulina Perlin, *Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance,* 25 March 2019, https://www.lawfareblog.com/newly-disclosed-nsa-documents-shed-further-light-five-eyes-alliance.

Sead Fadilpasic, *Paris hospitals targeted in major cyberattack*, 24 March 2020, https://www.itproportal.com/news/paris-hospitals-targeted-in-major-cyberattack/;

Sean Lawson, *Does 2016 Mark the End of Cyber Pearl Harbor Hysteria?*, 7 December 2016, https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#39dc0bed22c2:

Seth Djane Kotey, Eric Tutu Tchao, James Dzisi Gadze, 'On Distributed Denial of Service Current Defense Schemes' (2019), available at https://www.mdpi.com/2227-7080/7/1/19/htm.

Sherman, J., *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?*, Council on Foreign Relations, 30 October 2017, https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

Shira Stein, Jennifer Jacobs, *Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak*, 16 March 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

Sputnik News*, Estonia has no evidence of Kremlin involvement in cyber attacks*, 6 September 2007, https://sputniknews.com/world/2007090676959190/;

Statista, Stuxnet Infected Hosts By Country, https://www.statista.com/statistics/271110/stuxnet-infected-hosts-by-country/.

Statista, Worldwide digital population as of April 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/.

Stubbs, J., Menn, J., Bing, C., *Inside the West's failed fight against China's 'Cloud Hopper' hackers*, Reuters, 26 June 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

Sumi Somaskanda, *The Cyber Threat To Germany's Elections Is Very Real*, 20 September 2017, https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162/.

TechTerms, *Cyberspace Definition*, https://techterms.com/definition/cyberspace

The Guardian, *Prosecutors open homicide case after cyber-attack on German hospital*, 18 September 2020, https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital;

The International Committee of the Red Cross (ICRC), *The Potential Human Cost of Cyber Operations (*2018), https://reliefweb.int/sites/reliefweb.int/files/resources/the-potential-human-cost-of-cyber-operations.pdf.
The Local, *German experts see Russian link in deadly hospital cyber attack*, 22 September 2020, https://www.thelocal.de/20200922/german-experts-see-russian-link-in-deadly-hospital-hacking.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Croatian Prime Minister: Tallinn Manual is an Icebreaker*, 27 January 2015, https://ccdcoe.org/news/2015/croatian-prime-minister-tallinn-manual-is-an-icebreaker/.
UN Secretary General, *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.

UNESCO Glossary, *Information and Communication Technologies (ICT)*, http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict

United Nations Environment Programme (UNEP), 'IEG of the Global Commons: Background', available at https://cil.nus.edu.sg/wp-content/uploads/2015/12/Ses4-7.-UNEP-Division-of-Environmental-Law-and-Conventions-Global-Commons.pdf.

United Nations, Meetings Coverage and Press Releases, *First Committee Delegates Discuss Best Tools for Fighting Illegal Arms Trade, amid Calls to Boost Control of*

Conventional Weapons, 12 October 2018, https://www.un.org/press/en/2018/gadis3601.doc.htm

UNODA, *Fact Sheet on Developments in the Field of Information and Telecommunications in the Context of International Security*, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

UNODA, https://www.un.org/disarmament/ict-security/

Valentin Weber, *States and Their Proxies in Cyber Operations*, 15 May 2018, Lawfare, https://www.lawfareblog.com/states-proxies-cyber-operations.

William G. Rich, *The US Leans on Private Firms to Expose Foreign Hackers*, 29 November 2018, Wired, https://www.wired.com/story/private-firms-do-government-dirty-work/.

World Anti-Doping Agency, *WADA Confirms Attack by Russian Cyber Espionage Group*, 13 September 2016, https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group.

World Health Organization, News Release, *WHO reports fivefold increase in cyber attacks, urges vigilance*, 23 April 2020, https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

World Population Review, *Most Technologically Advanced Countries 2020*, https://worldpopulationreview.com/country-rankings/most-technologically-advanced-countries

YLE News, *DoS attack downs public service websites*, 22 August 2019, https://yle.fi/uutiset/osasto/news/dos_attack_downs_public_service_websites/10933436.

YLE Uutiset, *Suomi ollut tietoverkkohyökkäyksen kohteena*, 5 April 2020, https://yle.fi/uutiset/3-9548424