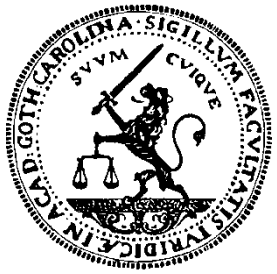

FACULTY OF LAW
Lund University

Victoria Bertilsson

Your Election, but Whose Choice?

A Study of the Applicability of the Principle of Non-intervention to Foreign Electoral Cyber Interference Aiming to Manipulate Voting Behaviour

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Markus Gunneflo

Semester of graduation: Period 1 Fall semester 2019

Contents

SUMMARY 1

SAMMANFATTNING 2

PREFACE 3

ABBREVIATIONS 4

1 INTRODUCTION 5

1.1 Background 5

1.1.1 Electoral Interference in the 2016 United States Election 5

1.1.2 The History of Electoral Interference 7

1.2 Purpose and Research Question 9

1.3 Delimitations 11

1.4 Method and Material 11

1.5 Research Situation 14

1.6 Terminology 15

1.7 Outline 16

2 WHAT IS ELECTORAL CYBER INTERFERENCE AIMING TO MANIPULATE VOTING BEHAVIOUR? 17

2.1 Methods of Electoral Cyber Interference Aiming to Manipulate Voting Behaviour 17

2.2 A Hypothetical Case of Voter Manipulation 19

3 THE DEFINITION OF THE PRINCIPLE OF NON-INTERVENTION 21

3.1 The Principle of Non-intervention 21

3.2 The Two Elements 24

3.2.1 Matter in which Each State is Permitted to Decide Freely 24

3.2.2 Coercion 25

3.3 Conclusions and Challenges 28

4 THE APPLICATION OF THE PRINCIPLE OF NON-INTERVENTION TO ELECTORAL CYBER INTERFERENCE AIMING TO MANIPULATE VOTING BEHAVIOUR 30

4.1 Non-intervention and Cyberspace 30

4.2 The Element of Coercion Regarding Attempts to Affect Voting Behaviour by Electoral Cyber Interference 31

4.2.1 Forcible Coercion Threatening of Consequences 33

4.2.2 Coercion Manipulating the Voters' Opinion Forming Environment 36
4.2.3 Concluding Summary 40
4.3 Criteria or a Holistic Approach? 41
4.4 The Different Approaches Applied to the Hypothetical Case 43
4.4.1 Forcible Coercion Threatening of Consequences 43
4.4.1.1 Using Criteria 43
4.4.1.2 Using a Holistic or Combined Approach 44
4.4.2 Coercion Manipulating the Voters' Opinion Forming Environment 46
4.4.2.1 Using Criteria 46
4.4.2.2 Using a Holistic or Combined Approach 46
4.5 Concluding Summary 48
4.6 The Future of the Criterion of Coercion 49
4.6.1 Including Electoral Cyber Interference Aiming to Manipulate Voting Behaviour in the Definition of Coercion 49
4.6.2 Replacing the Criterion of Coercion 51

5 FINDINGS AND CONCLUSIONS 53
5.1 The Exclusion of Electoral Cyber Interference Aiming to Manipulate Voting Behaviour from the Definition of the Principle of Non-intervention 53
5.2 Implications of the Definitions of Coercion 53
5.3 Potential Future and Inclusion in the Scope of the Principle of Non-intervention 54

BIBLIOGRAPHY 57

TABLE OF CASES 63

Summary

Electoral cyber interference aiming to manipulate voting behaviour is becoming increasingly sophisticated. This creates a risk of the interference undermining the trust in the democratic process with declining voter turnout as a result. The interference could also affect the outcome of elections.

The development of the technology enabling cyber voter manipulation is rapid, and international law lags behind. There are no wide-spread conventions or customary international law applicable to the specific situation. The general insecurity regarding the legality of cyber operations aiming to manipulate voting behaviour increases the risk of conflicts resulting from misunderstandings or misperceptions between states. To contribute to the clarification of the legality of voter manipulation, the purpose of this thesis is to analyse the legality of electoral cyber interference aiming to manipulate voting behaviour in relation to the principle of non-intervention. To achieve the purpose the critical argumentation method has been used.

While electoral cyber interference aiming to manipulate voting behaviour clearly fulfils the first criterion of non-intervention, by intervening in the *domaine réservé* of another state, the fulfilment of the second criterion, coercion, is more complicated. The criterion of coercion is not fully defined in international law, but is traditionally described as forcible or dictatorial coercion compelling a state to involuntarily act or refrain from acting with non-abidance resulting in consequences. In this definition, electoral cyber interference aiming to manipulate voting behaviour does not fulfil the criterion of coercion. A different interpretation of the criterion of coercion is the definition of coercion as the manipulation of the environment in which the voters form their opinion to thereby exercise control over the voters. This definition has been suggested to make the criterion of coercion more adapt to the modern technological development, and to include voter manipulation. However, the support of this more modern interpretation is scarce. As a result of this, the correct definition of the criterion of coercion should be forcible or dictatorial coercion. Therefore, electoral cyber interference aiming to manipulate voting behaviour is not a violation of the principle of non-intervention due to the lack of coercion.

Despite voter manipulation not constituting a prohibited intervention today, a prohibition could facilitate the protection of free elections and thereby state sovereignty. A development of the scope of the principle of non-intervention, either by widening the definition of the criterion of coercion or by replacing it, could be a practical and efficient solution.

Sammanfattning

Elektronisk valpåverkan med syfte att manipulera väljarbeteenden blir allt mer sofistikerad vilket medför en risk för att valpåverkan underminerar förtroendet för den demokratiska processen och därmed påverkar valdeltagandet negativt. Valpåverkan kan eventuellt också påverka valresultatet.

Den teknologiska utvecklingen som möjliggör elektronisk valpåverkan är snabb och den internationella rätten hänger inte med. Det finns inte några omfattande konventioner eller sedvanerätt som är applicerbar på situationen. Den generella osäkerheten angående lagligheten av elektronisk valpåverkan ökar risken för konflikter till följd av missförstånd eller missuppfattningar mellan stater. För att bidra till att klargöra rättsläget är syftet med den här undersökningen att analysera lagligheten av elektronisk manipulation av väljarbeteenden i förhållande till principen om non-intervention. För att uppnå syftet har en kritisk argumentationsanalys använts.

Elektronisk valpåverkan med syfte att manipulera väljarbeteenden uppfyller tydligt det första rekvisitet för non-intervention, genom att ingripa i frågor inom en annan stats *domaine réservé.* Huruvida det andra rekvisitet, tvång, uppfylls är mer tveksamt. Tvångsrekvisitet har inte definierats utförligt i internationell rätt, men har traditionellt beskrivits som kraftfullt och diktatoriskt tvång som förmår en stat att ofrivilligt agera eller inte agera på ett visst sätt och där olydnad leder till konsekvenser. Med den här definitionen uppfyller elektronisk valpåverkan med syfte att manipulera väljarbeteenden inte tvångsrekvisitet. En annan tolkning av tvångsrekvisitet är att manipulation av miljön i vilken väljarna formar sina åsikter är tvång då väljarnas röster genom manipulationen kontrolleras. Tolkningen har föreslagits som mer anpassad till den moderna teknologiska utvecklingen, däribland väljarmanipulation. Stödet för denna mer moderna tolkning är dock relativt svagt. Den korrekta definitionen av tvångsrekvisitet bör därför anses vara kraftfullt och diktatoriskt tvång. Det innebär att elektronisk valpåverkan med syfte att manipulera väljarbeteenden, till följd av bristen på tvång, inte strider mot principen om non-intervention.

Trots att elektronisk manipulation av väljarbeteenden således inte strider mot principen om non-intervention idag, så skulle dock ett förbud kunna stärka skyddet för fria val och därmed också stärka staters suveränitet. En utveckling av tillämpningsområdet för principen om non-intervention, antingen genom att bredda eller ersätta tvångsrekvisitet, skulle kunna vara en praktisk och effektiv lösning.

Preface

I would like to express my sincerest gratitude to my supervisor Markus Gunneflo. Thank you for sharing your thoughts with me and guiding me through this process, despite my sometimes faltering long-term planning.

Thank you, Erica, Marija and Simon, for proof reading and making this thesis better.

Thank you, Henna, for keeping me sane during this writing process. Or at least keeping me company in this insanity.

To Vältarna (close or far away in time and space), Flexitariatet and all the rest of you that have made this time in Lund a period of my life that I warmly and reminiscently will talk about for decades to come, thank you.

To my family, thank you for the love, support and for always being my safe haven. Lanka, thank you for, when in doubt, always reminding me of who I am. Mamma, there are not enough words. So I will simply say this: If I ever become half the person that you are, I can never ask for anything more.

Lund, January 2020

Victoria Bertilsson

Abbreviations

DDoS	Distributed denial-of-service
DNC	Democratic National Committee
Friendly Relations Declaration	UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 24 October 1970, A/RES/2625(XXV)
ICJ	International Court of Justice
ICJ Statute	Statute of the International Court of Justice
IRA	Internet Research Agency
NATO	North Atlantic Treaty Organization
Nicaragua-case	*Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua v. United States of America) (Merits) [1986] ICJ Rep 14
OAS Charter	Charter of the Organization of American States
OAU Charter	Charter of the Organisation of African Unity
PCIJ	Permanent Court of International Justice
UN Charter	United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI
UNGA	United Nations General Assembly
USSR	Union of Soviet Socialist Republics

1 Introduction

1.1 Background

A version of a principle of non-intervention has existed for a long time and the idea was first mentioned by Christian Wolff and Emmerich de Vattel in the 18th century.[1] The concept has since then developed, and today the principle prohibits coercive intervention in the internal or external affairs of other states, which include the conduction of national elections. One of the ways to interfere in elections is by manipulating the voting behaviour. The introduction of the internet has created a new arena for electoral interference by manipulating voting behaviour. The technological possibilities are rapidly developing and the methods available to affect the outcomes of elections are becoming more sophisticated.

1.1.1 Electoral Interference in the 2016 United States Election

An illustrative example of electoral cyber interference aiming to manipulate voting behaviour was the alleged Russian interference in the 2016 United States election.[2] The purpose of the interference was to discredit the democratic presidential candidate Hillary Clinton, to favour the republican candidate Donald Trump and to undermine the faith of the public regarding the democratic process in the United States in general.[3]

The Russian cyber influence campaign was multifaceted and included several methods of interference, including the hacking and leaking of documents, propaganda campaigns in different media outlets and 'trolling' on social media.[4]

An example of a hack-and-leak operation was the hack of the email system of the Democratic National Committee (DNC) and its officials in March

[1] Chen Yifeng, 'The Customary Nature of the Principle of Non-Intervention: A Methodological Note' (2014) 2 Renmin Chinese L Rev 319, 333.
[2] Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law' (2017) 95 Tex L Rev 1579, 1579.
[3] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Election*. (Intelligence Community Assessment 6 January 2017) 1, 4 <https://www.dni.gov/files/documents/ICA_2017_01.pdf> accessed 5 January 2020.
[4] The Office of the Director of National Intelligence (n 3) 2; Michael N Schmitt, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 Chi J Int'l L 30, 34.

2016. The emails and other material were spread through hacker personas, a number of websites such as DNCLeaks.com and WikiLeaks as well as through media releases.[5] The leak of nearly 20 000 emails resulted in an outrage as the emails revealed that the DNC (which professed itself neutral) favoured Clinton as the Democrat's presidential candidate over Bernie Sanders.[6] The release of the information coincided with the Democratic nomination convention and forced the DNC's chairwoman to resign.[7] A second batch of emails were also released at a critical time, a few days before the election.[8] The chairman of Clinton's presidential campaign, John Podesta, also had his emails leaked. The emails were released an hour after the newspaper Washington Post published a tape of Trump degradingly commenting about women.[9]

Simultaneously, Russia launched a classic propaganda campaign through various media outlets including *RT* (former *Russia Today*) and *Sputnik*. To this the social media activities of the trolls of the Russian Internet Research Agency (IRA) were added.[10] The IRA constituted of hundreds of paid trolls.[11] The trolls spread advertisements to a cost of more than two million dollars, created more than 120 social media groups and accounts and encouraged more than forty rallies and campaigns to convince the United States voters to vote for Trump and not Clinton, but also to keep people from voting through statements such as 'Hillary Clinton doesn't deserve the black vote!'.[12] Some trolls posed as American citizens, either by fake personas or impersonating existing Americans and some went as far as travelling to the United States to conceal the origin of the cyber operation by using American infrastructure.[13] Besides the trolls, bots (a software program performing automatic tasks on the internet) are estimated to automatically have produced one in seven of the political tweets during the election campaign.[14]

---

[5] Ohlin (n 2) 1579; Schmitt 'Virtual Disenfranchisement' (n 4) 2-3.
[6] Ido Kilovaty, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information' (2018) 9 Harv Nat'l Sec J 146, 149.
[7] Logan Hamilton, 'Beyond Ballot-Stuffing: Current Gaps in International Law regarding Foreign State Hacking to Influence a Foreign Election' (2017) 35 Wis Int'l LJ 179, 180.
[8] Kilovaty (n 6) 155-156.
[9] Kilovaty (n 6) 156.
[10] Schmitt 'Virtual Disenfranchisement' (n 4) 34.
[11] Shaun Walker, 'The Russian troll factory at the heart of the meddling allegations' *The Gaurdian* (St Petersburg 2 April 2015) <https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house> accessed 4 January 2020.
[12] Schmitt 'Virtual Disenfranchisement' (n 4) 35.
[13] Schmitt 'Virtual Disenfranchisement' (n 4) 36.
[14] Martin Moore, *Democracy hacked: political turmoil an information warfare in the digital age* (Oneworld Publications 2018) 100-101.

The effect of the interference in the United States election is not verified, but there are studies claiming that the interference could have been the determining factor for the narrow victory of Trump. A correlation has been found between belief in fake news stories supporting Trump and discrediting Clinton, and the defection of voters from the Democratic party who voted for Barack Obama but not Clinton.[15]

The United States is not the only state that has claimed to have been victim of electoral cyber interference aiming to manipulate voting behaviour.[16] Other examples are the Brexit referendum, the elections of France, Spain, Italy and the Baltic states, and political and party websites in in Germany, Norway and Denmark.[17] Russia is often pointed out as the perpetrator, but has also claimed to be a victim of electoral cyber interference, originating from locations in fifteen states, during the 2018 presidential election.[18] Several states have also been taking advantage of the internet's development. In 2017 it was estimated that twenty-eight states had engaged in some form of social media manipulation and the number is likely to increase.[19]

1.1.2 The History of Electoral Interference

Attempts to interfere in foreign elections is a phenomenon far predating the development of the internet and have frequently been made since the rise of meaningful competitive elections.[20] During the period from 1946 to 2000 the United States and the Union of Soviet Socialist Republics (USSR)/Russia intervened in 117 (one out of every nine) competitive national level executive elections.[21] Frequent targets of American electoral interference was Latin America, including Guatemala, Chile and Nicaragua.[22] Not only the great powers, but smaller states also tried to influence the outcome of foreign elections, both in their own regions and in the great powers themselves.[23]

---

[15] Richard Gunther, Paul A. Beck, Erik C. Nisbet, *Fake News May Have Contributed to Trump's 2016 Victory* (March 8 2018 Ohio State University) 2. <https://assets.documentcloud.org/documents/4429952/Fake-News-May-Have-Contributed-to-Trump-s-2016.pdf> accessed 14 December 2019.
[16] Schmitt 'Virtual Disenfranchisement' (n 4) 32, 36-37.
[17] Schmitt 'Virtual Disenfranchisement' (n 4) 37; Moore (n 14) 72-74.
[18] Schmitt 'Virtual Disenfranchisement' (n 4) 37.
[19] Moore (n 14) 103.
[20] D. H. Levin, 'A Vote for Freedom? The Effects of Partisan Electoral Interventions on Regime Type' (2019) 63 *JCR 839,* 839.
[21] Dov H. Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (2016) 60 ISQ 189, 191.
[22] Schmitt 'Virtual Disenfranchisement' (n 4) 38.
[23] Lori Fisler Damrosch, 'Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83 Am J Int'l L 1, 2.

Traditionally, political and electoral interference have commonly been combined with forcible intervention.[24]

The methods of electoral interference utilized varied from public threats or promises made by an official of the interfering state to funding or providing campaign material of the preferred candidate.[25] An example of the latter is the USSR's support in the 1972 West German parliamentary election.[26] Other methods were affirmative tools of leverage such as the award of economic benefits, government-to-government aid and preferential trade relations.[27] The still relevant interference method of propaganda was historically performed through newsletter bombings, radio broadcasts and loudspeakers near the border, as by the South and North Korean border.[28]

Much of the support to candidates was given through intermediates to conceal the origin of the support. The intermediate could be a labour union, business organization, the press or other ostensibly private groups. More creative methods to conceal the origin of funds have been the USSR's funding of the Italian Communist Party (a third of the party's expenditure) through profits or commissions from party-run enterprises involved in trade or tourist ventures with the USSR.[29]

Another example of historical intervention, that is still relevant today, is 'dirty tricks', for example creating and leaking forged documents to create the vision of misdeeds by a candidate.[30] The hacking and subsequent leaking of authentic but confidential documents is also not a new phenomenon. It was used in 1956, when the United States obtained and leaked a copy of the USSR leader Nikita Khrushchev's upcoming speech in which he denounced the atrocities which had taken place during the former USSR leader Joseph Stalin's lead.[31]

Interference in support of a certain candidate during the period 1946 to 2000 may have had a significant impact on the aided candidate's chance to get

[24] Fisler Damrosch (n 23) 4.
[25] Levin 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 192-193.
[26] Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 199-200.
[27] Fisler Damrosch (n 23) 28-29.
[28] Ohlin (n 2) 1588.
[29] Fisler Damrosch (n 23) 15.
[30] Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 192-193.
[31] Kilovaty (n 6) 157.

elected. According to one study, the average effect of the interference was three percent, which often can be enough to swing elections.[32]

There is no indication of state interest in electoral interference reducing.[33] Instead, partisan electoral interference is likely to become even more common in a world where military interventions are increasingly costly and democracies more common.[34]

1.2 Purpose and Research Question

In international relations, it has always been beneficial for a state to have other states led by persons with favourable dispositions towards them. Consequently, states have frequently tried to install such governments or support preferred candidates in other states' elections. While the history of states trying to interfere in other states' elections is as old as democratic elections themselves, the technical developments resulting from the introduction of the internet have made such attempts more convenient. The effect of electoral interference has increased as a result of increased scalability due to the cost efficiency, anonymity, instantaneous cross-border effect and accessibility of the internet as well as the variety of means and methods available. Today, a popular method frequently used by states to influence the outcome of an election in another state is electoral cyber interference with the aim to manipulate the voting behaviour of the voters in the target state. As states develop technologically and more potential voters get access to the internet, the states' vulnerability to such electoral interference increases.

Besides the risk that a candidate is elected, that would not have been elected without the interference, infringing the sovereignty of the target state, there are other potential negative effects of cyber voter manipulation. Electoral interference risk undermining the trust in the democratic process due to the foreign influence.[35] This can subsequently lead to reduced participation in elections, either by a specific group or by the voters in general.[36] Furthermore,

---

[32] Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 199-200.
[33] Daniel Corstange and Nikolay Marinov, 'Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention (2012) 56 AJPS 655, 655.
[34] Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 201.
[35] Cf. 'Methods of Foreign Electoral Interference' (*EUvsDisinfo,* 2 April 2019) <https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/> accessed 2 January 2020.
[36] Chris Tenove and others, 'Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy' (Centre for the Study of Democratic Institutions, UBC January 2018) 26-27.

the interference can shift focus from issues of general interest for the public to less relevant or non-existing issues as well as weakening the understanding of public issues and spreading disagreement.[37]

While the internet and the technological possibilities of electoral cyber interference is rapidly developing, international law lags behind. Neither international treaties nor customary international law has been able to meet the demand for up to date regulations. Instead, the legal debate has mainly been focusing on applying existing international law to the new arena of cyberspace. Regarding electoral cyber interference aiming to manipulate voting behaviour, the legal norm generally considered most probable to be applicable, is the principle of non-intervention.[38] Therefore, the principle of non-intervention will be the main focus of this thesis.

The general insecurity regarding the legality of cyber operations aiming to manipulate voter behaviour increases the risk of conflict resulting from misunderstandings or misperceptions between states. To reduce the risk of such conflict, it is important to clarify the legal situation.[39] Therefore, to provide legal clarity, the purpose of this thesis is to analyse the legality of electoral cyber interference aiming to manipulate voting behaviour in relation to the principle of non-intervention.

To achieve this purpose, the following questions will be answered:

- *How is the principle of non-intervention defined?*

- *Can electoral cyber interference by one state, aiming to manipulate the voting behaviour of the voters in the target state, constitute a violation of the principle of non-intervention?*

    - *Especially, how is the criterion of coercion, which is required for an act to constitute a violation of the principle of non-intervention, defined?*

<https://democracy2017.sites.olt.ubc.ca/files/2018/01/DigitalThreats_Report-FINAL.pdf> accessed 9 December 2019.

[37] Tenove (n 36) 28.

[38] Cf. Kilovaty (n 6); Schmitt 'Virtual Disenfranchisement' (n 4); Nicholas Tsagourias 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' (EJIL: Talk!, 26 August 2019) <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/#more-17430> accessed 4 December 2019.

[39] Cf. Patryk Pawlak, 'Confidence-Building Measures in Cyberspace: Current Debates and Trends' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016) 130.

    - *What are the implications of different definitions of the criterion of coercion?*

- *If electoral cyber interference by one state, aiming to manipulate the voting behaviour of the voters in the target state, cannot constitute a violation of the principle of non-intervention, should such interference be possible to constitute a violation of the principle of non-intervention?*

The first question will be answered in the third chapter. The second and third questions, including the sub-questions, will be answered in the fourth and fifth chapter.

1.3 Delimitations

The legality of electoral cyber interference aiming to manipulate voting behaviour can be analysed in relation to a number of different legal norms, including the right to self-determination, sovereignty and the human right to privacy.[40] However, the principle of non-intervention is in general considered most likely to be applicable to voter manipulation and the analysis in this thesis will therefore be limited to the application of that principle.

While the possibilities of affecting voting behaviour are many, this thesis will only encompass voter manipulation taking place in cyberspace. More tangible forms of interference, such as the hacking and manipulation of voting equipment or the counting of votes, is also outside the scope of this thesis.

One of the benefits of an interfering state of using cyber means to interfere in elections is the anonymity and the difficulties of establishing the origin of the cyber operations. The attribution issue is made further challenging by the fact that the attacks generally are executed by intermediates such as groups of hackers. The question of attribution is, however, not within the scope of this thesis.

1.4 Method and Material

The definition of the principle of non-intervention in chapter three is a determination of established law and the doctrinal research method has therefore been used. The doctrinal research method is based on the utilization

[40] Schmitt 'Virtual Disenfranchisement' (n 4).

of the traditional sources of international law which, according to Article 38(1) of the Statute of the International Court of Justice (ICJ Statute), are international conventions, international customary law and general principles. Judicial decisions and the teachings of the most highly qualified publicists are subsidiary means for determining the rules of law.

The principle of non-intervention is mentioned in several international documents, for example regional treaties such as *the Charter of the Organization of American States* (*OAS Charter*)[41] and the *Charter of the Organisation of African Unity* (*OAU Charter*)[42] among others. Due to the lack of a global legally binding treaty including the principle, the principle's main significance originates from it being a part of customary international law. To define the scope of the principle of non-intervention, regional treaties, United Nations General Assembly (UNGA) resolutions, case law from the International Court of Justice (ICJ) and the Permanent Court of International Justice (PCIJ) and legal literature, will be considered. The most indicative case law regarding the principle of non-intervention is the *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua-case)* from the ICJ.[43] Due to the shortage of more primary sources of law concerning the general definition of the principle of non-intervention, legal literature will be the main source.

Before the general definition of the principle of non-intervention, in chapter two, a variety of methods of electoral cyber interference aiming to manipulate voting behaviour are presented. Despite the methods being quite many, they are only examples of methods utilized and new methods are constantly being developed. The examples have been chosen to illustrate the most common methods of cyber voter manipulation used today, but also to present the width of methods available. The examples of methods are subsequently used to create a hypothetical case of large-scaled electoral cyber interference aiming to manipulate voting behaviour. The hypothetical case is created to be a large-scaled and multifaceted interference (though still within the boundaries of what is possible) even though no such exact manipulation operation is publicly known today. The hypothetical case is presented early on in the thesis to provide a background and an understanding of the challenges with the definition of the principle of non-intervention.

[41] Organization of American States (OAS), Charter of the Organisation of American States, 30 April 1948.
[42] Organization of African Unity (OAU), Charter of the Organization of African Unity, 25 May 1963.
[43] (Nicaragua v. United States of America) (Merits) [1986] ICJ Rep 14.

In chapter four, the critical argumentation method will be used to analyse the arguments found in the legal literature and assess the legality of cyber voter manipulation in relation to the principle of non-intervention. The objective of the critical argumentation method is to impartially and reasonably evaluate the strengths and weaknesses of arguments.[44] This is obtained through three steps, identifying, analysing and evaluating the arguments. A successful argument is one that give good reason, or several reasons, to support or criticize a claim.[45] The critical argumentation will be based on a typology where different definitions of the criterion of coercion, upon which non-intervention is based, are identified, separated into two categories based on the understanding of the concept of coercion, analysed and evaluated. The identification of different arguments will therefore throughout chapter four be followed by my analysis and evaluation. The categories of coercion, and thereby non-intervention, are subsequently applied to the hypothetical case from chapter two, to illustrate the differences and outcomes of the application of the definitions. The consequences of choosing the different definitions of coercion are analysed and evaluated.

Since international law lags behind the technological development that makes electoral cyber interference aiming to manipulate voting behaviour possible, the law is unclear regarding the definition of the principle of non-intervention and its application to such interference. The very few treaties applicable to cyber operations are of limited scope and can therefore in general not be applied. Furthermore, it is difficult to determine the scope of the customary principle of non-intervention in the context of voter manipulation due to the lack of state practice and indications of *opinio juris*. The shortage can, besides be explained by the phenomenon being new, partly be explained by information regarding cases of voter manipulation generally being classified, both in the interfering and the target state. Hence, no cyber specific customary international law has currently been specified.[46] Neither has there been any cases before an international court. Therefore, the main source in the critical argumentation will be legal literature, where the most common approach is to apply already existing international law to the new arena of cyberspace and identify cyber-specific aspects.[47]

---

[44] Douglas N. Walton, *Informal logic: a handbook for critical argumentation* (Cambridge University Press 1989) 1.
[45] Douglas N. Walton, *Fundamentals of Critical argumentation* (Cambridge University Press 2006) 1.
[46] Michael N. Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016) 46; Michael N. Schmitt and Liis Vihul (ed), *Tallinn manual 2.0 on the international law applicable to cyber operations: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence* (2nd edn, Cambridge University Press 2017) 3.
[47] Cf. Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 3.

The means needed to, by cyber means, interfere in other states' elections by manipulating voting behaviour has only existed for a brief period of time. Hence, the legal literature on the topic is still somewhat limited. This has reduced the need of selection criteria regarding the legal arguments to be analysed. Almost all arguments in trustworthy journals or other literature, made by legal scholars and scholars of other relevant subjects, have been included in the thesis. There are, however, only a few publications in which the application of the principle of non-intervention is exhaustively discussed.

However, the source languages used, mainly English and Swedish, have limited the source material. This has also resulted in the majority of the used legal literature originating from authors in the western hemisphere (frequently the United States). This may have resulted in a western perspective on the matter and may be a reason for Russia (rightfully or unrightfully so) frequently being pointed out as the alleged perpetrator of cyber voter manipulation. The United States' centric discourse of the rule of law in cyberspace, especially concerning the militarization of cyberspace, has been criticized.[48]

1.5 Research Situation

Despite the principle of non-intervention being dealt with extensively in legal research, there is no exact definition of the principle. The principle is often mentioned in the context of the prohibition of the use of force, as in *Oppenheim's International Law* by L. Oppenheim from 1996 and Malcolm N Shaw's *International law* from 2017. An article examining non-forcible intervention is the 2009 article *Current Legal Developments: The Principle of Non-intervention* by Maziar Jamnejad and Michael Wood which conclude that some, but not all forms of non-forcible interference can be violations of the principle of non-intervention. Already in 1989, Lori Fisler Damroch pointed out the problem of interference affecting elections falling out of the scope of the principle of non-intervention in her article *Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs*. Damrosch also called for a redefinition of the criterion of coercion to widen the scope of the principle of non-intervention.

One of the publications frequently referred to regarding the law of cyber operations is the 2017 *Tallinn Manual 2.0 on the International Law*

[48] Kristin Bergtora Sandvik, 'Law in the militarization of cyber space: framing a critical research agenda' in Karsten Friis and Jens Ringmose (eds), *Conflict in cyber space: theoretical, strategic and legal perspectives* (Routledge 2016) 175.

Applicable to Cyber Operations. In the Manual, international law experts have applied existing international law to cyber operations. The main focus of the manual is *jus ad bellum* and *jus in bello*, but key aspects of the law concerning cyber operations in peacetime are also examined. Though briefly mentioned, it is concluded in the manual that the principle of non-intervention is not applicable to cyber voter manipulation.

While most of the research regarding the application of the principle of non-intervention to electoral cyber operations concern cyber operations including the use of force, there are some exceptions. In the 2018 article *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information* Ido Kilovaty concludes that hack-and-leak operations most likely does not constitute a violation of the principle of non-intervention and calls for replacing the criterion of coercion with a criterion of disruption.

The criterion of coercion is central in most research regarding the application of the principle of non-intervention, though the conclusions regarding whether cyber voter manipulation can amount to coercion or not is inconclusive. In his 2015 article, *Did Russian Cyber Interference in the 2016 Election Violate International Law?,* Jens David Ohlin concluded that electoral cyber interference aiming to manipulate voting behaviour does not violate the principle of non-intervention due to its lack of coercion. Contrastingly, Nicholas Tsagourias in his 2019 work *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace* conclude that electoral cyber interference aiming to manipulate voting behavior can be coercive and violate the principle of non-intervention.

The research on the applicability of the principle of non-intervention to large-scaled electoral cyber interference aiming to manipulate voting behaviour is relatively scarce. The research that exists today generally either focus on one type of cyber voter manipulation or only discuss the applicability of the principle of non-intervention briefly. Hopefully, this thesis can contribute to the field of research regarding the applicability of the principle of non-intervention to large-scaled electoral cyber interference aiming to manipulate voting behaviour.

1.6 Terminology

The terms *intervention* and *interference* are frequently used interchangeably in legal research regarding the principle of non-intervention. This is, however, considered a mistake by some researchers. Interference is acts which intend

to meddle in matters within the internal or external affairs of another state but lack coercion or use of force. Interference is, in contrast to intervention, not a violation of international law.[49] A similar interpretation is going to be used in this thesis. The term interference will be used for attempts to influence or manipulate voting behaviour that fall short of being interventions due to the lack of coercion, or in cases where it has yet to be analysed whether the act reaches the threshold of coercion and thereby intervention. The term intervention will only be used regarding actions which are considered to be violations of the principle of non-intervention.

1.7 Outline

The second chapter will commence with an illustration and explanation of different methods of electoral cyber interference aiming to manipulate voting behaviour. The methods are subsequently used to create a hypothetical case of large-scaled cyber voter manipulation. The hypothetical case will be further used in chapter four.

In the third chapter the general principle of non-intervention in analysed and defined. Political interference will due to the theme of the thesis receive special attention. The chapter concludes with observing the challenges of applying the general definition of non-intervention to electoral cyber interference aiming to manipulate voting behaviour.

The fourth chapter will focus on the potential applicability of the principle of non-intervention to electoral cyber interference aiming to violate voting behaviour. Emphasise will be put on defining the criteria of coercion in the context of voter manipulation. The different potential definitions of coercion will be categorized and analysed based on merits and disadvantages. To illustrate the implications of different definitions of coercion, the definitions will be applied to the hypothetical case constructed in chapter two.

The fifth chapter concludes the thesis with a discussion of the applicability of the principle of non-intervention to cyber voter manipulation, the implications of different definitions of coercion and the possible future of the principle of non-intervention.

[49] Terry D. Gill, 'Non-intervention in the Cyber Context' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publication 2013) 217; Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 313; Kilovaty (n 6) 167.

2 What is Electoral Cyber Interference Aiming to Manipulate Voting Behaviour?

2.1 Methods of Electoral Cyber Interference Aiming to Manipulate Voting Behaviour

As illustrated in the background,[50] the efforts to influence the outcome of other states' elections by manipulating the opinion of the voters have existed for a long time. What is new, is the methods used and the means available. The technology is constantly developing, and so are the methods of interference.

A variety of different methods can be used to interfere and manipulate voting behaviour by cyber means: the hacking and leaking of confidential information, disinformation campaigns, trolling on social media, online propaganda, identity falsification and distributed denial-of-services attacks (DDoS-attacks) against websites (flooding a network resource by incoming traffic to make it unavailable to the legitimate users).[51] Both private and government internet infrastructure can be the target of voter manipulation operations.[52]

A classic method of interference still used today (but through the medium of the internet) is propaganda.[53] A method related to propaganda is disinformation. Disinformation involves information, for example news, which are fabricated or deliberately distorted to deceive the audience, obscure a fact-based reality and undermine the trust in the democratic process.[54] The internet has made the spread of disinformation campaigns and propaganda more pervasive and large social media platforms such as Google, Facebook

[50] Ch 1.1.2.
[51] Kilovaty (n 6) 147; Schmitt 'Virtual Disenfranchisement' (n 4) 52; 'Methods of Foreign Electoral Interference' (n 35).
[52] Schmitt 'Virtual Disenfranchisement' (n 4) 48.
[53] Ohlin (n 2) 1588.
[54] 'Methods of Foreign Electoral Interference' (n 35).

and Twitter have been criticized for not being active enough in countering the disinformation.[55]

The spread of disinformation and propaganda is often combined with sentiment amplification where fake accounts, trolls or automated bots are used to spread the disinformation and propaganda on social media and comment sections. The aim of sentiment amplification is to promote a specific narrative while creating further confusion regarding facts and reducing the trust in the democratic process. The narrative can also be spread by political advertising where fake or non-tracible identities and accounts are used to purchase online political ads where disinformation is used to promote the favoured candidate and disfavour the opponents.[56]

To make the propaganda and disinformation more effective, the messages can also be customized to different groups of voters. This method was famously used by the political data firm Cambridge Analytica. By taking a quiz in an app, the users consented to the app getting access to their Facebook profile and the profiles of their friends. Through the app the creators got access to the full profile of 50 million accounts. The profile information was (after being matched with other records) used to construct personality profiles of 30 million voters. The classifications were subsequently sold to be used to better influence the voters by psychographic modelling techniques.[57] Improving the targeting of specific groups has also been done by the use of algorithms (decision-making code).[58]

As seen in the background[59], the leaking of information for political benefits is not a new concept, but the internet has made the process more effective.[60] The terms hack-and-leak operations or doxing have been used to describe state sponsored hacking into other states' networks and computer systems to retrieve confidential data, subsequently leaking selected documents to the public at strategic times to create the biggest impact.[61] The information is frequently published on internet platforms that can store a large amount of information, such as WikiLeaks.[62] The leaked documents can either be authentic but confidential or manipulated (or a combination) and the aim is to

---

[55] Kilovaty (n 6) 178.
[56] 'Methods of Foreign Electoral Interference' (n 35).
[57] 'Cambridge Analytica' (Geneva internet platform, DigitalWatch Observatory) <https://dig.watch/trends/cambridge-analytica> accessed 12 December 2019.
[58] Samuel C. Woolley and Philip N. Howard (eds), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford University Press 2018) 6-7.
[59] Ch 1.1.2., 8.
[60] Kilovaty (n 6) 151.
[61] Kilovaty (n 6) 151-153; 'Methods of Foreign Electoral Interference' (n 35).
[62] Kilovaty (n 6) 154.

undermine a certain candidate or party.[63] The hacking is generally covert to make the question of attribution more complicated but the leak is overt to reach as many of the voters as possible.[64] The method utilized to retrieve the information from the targeted state's computer system can either be identity falsification or finding and using the vulnerabilities in the system to get access to the information (traditional hacking).[65]

Besides using identity falsification to prevent attribution when spreading disinformation and inciting a public reaction it can also be used to get hold of passwords and credentials by so called spear-phishing. [66] Spear-phishing are emails requesting confidential information, sent from a hacking group, appearing to originate from a trustworthy source but in reality having a malign intent such as making the receiver click on a link that will give the hacking group access to credentials.[67] The credentials are then used in order to conduct a cyber operation, such as hack-and-leak operations, by impersonating a specific individual.[68] Identity falsification can also be used to forge, or alter in a significant way, messages and information which are pretended to be originating from a party or candidate.[69]

DDoS-attacks can also be used in purpose of manipulating voting behaviour. DDoS-attacks involve large networks of hijacked, compromised computers (so called botnets), used by hackers to generate a huge amount of messages or logon requests to a specific internet address in order to overwhelm it so the internet address shuts down.[70] DDoS-attacks can be used to shut down a party website, blog, email or other online services used for campaigning during a critical point of the campaign process.[71]

2.2 A Hypothetical Case of Voter Manipulation

State A has an upcoming national election with two main candidates, from two opposing parties, candidates X and Y, with approximately equal support. State B strongly favours candidate X due to her favourable disposition

[63] 'Methods of Foreign Electoral Interference' (n 35).
[64] Kilovaty (n 6) 153.
[65] Kilovaty (n 6) 153.
[66] 'Methods of Foreign Electoral Interference' (n 35).
[67] Moore (n 14) 97.
[68] 'Methods of Foreign Electoral Interference' (n 35).
[69] Schmitt 'Virtual Disenfranchisement' (n 4) 52.
[70] George Lucas, *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare* (Oxford University Press 2017) 4.
[71] Schmitt 'Virtual Disenfranchisement' (n 4) 52.

towards state B. State B therefore attempts to manipulate the voting behaviour of the voters in state A to get candidate X elected.

State B launches an extensive disinformation campaign where information is distorted to obscure the perceived reality of the voters in support of candidate X and discrediting candidate Y. The campaign also attempts to weaken candidate Y's supporters' trust in the democratic process to reduce their voter turnout. State B uses political advertising and propaganda on social media and other platforms to support candidate X and further discredit candidate Y. Both the political advertising and disinformation campaign is launched by fake, non-tracible personas and personas imitating citizens of state A. State B's narrative is strengthen by the disinformation and propaganda which is further spread by sentiment amplification by trolls and bots on social media and different comment sections.

To magnify the effect of the influence campaign, it is customized for different groups of voters in state A and the content differs depending on the personality profiles of the different groups. The personality profiles have been created and bought from a private company.

The imitation of specific persons in state A is performed to attain passwords and credentials through spear-phishing. The credentials are subsequently used to hack into the computer systems of candidate Y and her campaign and retrieve confidential information. Selected documents are released at strategic times, sometimes with minor manipulation which state B hopes will go unnoticed. The identity falsification is also used to post messages pretending to be representatives of candidate Y to discredit candidate Y and lessen her support.

State B performs DDoS-attacks against candidate Y's campaign website and other websites supporting candidate Y at critical points of time during the campaign, such as after debates when many voters wish to fact-check statements regarding candidate Y.

Come election day, candidate X wins the election with a small margin. State B is publicly accused of having interfered but denies all allegations. It is not clear what effect the interference of state B had on the election result.

3 The Definition of the Principle of Non-intervention

3.1 The Principle of Non-intervention

The principle of non-intervention is frequently used in political rhetoric, but this must be distinguished from cases where non-intervention is used as a legal argument.[72] The principle has been defined as forcible or directorial interference by one state, in the affairs of another state, with the goal to impose certain conduct or consequences on the target state. The interference can be in the internal or external affairs of the target state and the effect on the affairs may be either direct or indirect.[73] The principle of non-intervention is only applicable on intervention between states.[74] The ICJ elaborated on the definition of the principle in the *Nicaragua-case.* In relation to the resolution of the case, the principle was in the judgement defined as:

> *The principle forbids al1 States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.*[75]

The case was brought before the ICJ against the United States by Nicaragua, claiming that the United States unlawfully had used force against the government of Nicaragua and that the United States had supported military and paramilitary activities by the opposition Contra's forces. In the judgement

[72] Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention' (2009) 22 LJIL 345, 347.
[73] L. Oppenheim, *Oppenheim's International Law: Peace,* vol 1 (Robert Jennings and Arthur Watts eds, 9th edn, 1996) 430.
[74] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 313.
[75] *Nicaragua-case* (n 43) para 205.

the content of the principle of non-intervention is considered and the quoted provision provides an authoritative statement regarding the scope of the principle of non-intervention. Despite frequent examples of violations of the principle of non-intervention, the court considered that the principle is part and parcel of customary international law. The court based its conclusion on inter alia the *Corfu Channel case*,[76] UNGA resolutions and inter-American practice.[77]

Customary international law is based upon state practice and *opinio juris.* It therefore requires states to, in general, behave in accordance with the principle but also to behave in that way due to the existence of a psychological element of the states actually believing that such behaviour is required by law.[78] The fact that the principle of non-intervention occasionally is violated does, as stated in the *Nicaragua-case*, not change the fact that such a prohibition exists. Interventions are generally considered illegal by states and are frequently condemned, which shows the existence of *opinio juris*.[79]

The principle of non-intervention is founded upon the concept of respect for the territorial sovereignty of states.[80] *The Charter of the United Nations* (*UN Charter*)[81] does not contain a specific provision concerning the principle of non-intervention, but the principle is reflected in Article 2(1) according to which: 'The Organization is based on the principle of the sovereign equality of all its Members'. The article establishes the principle of sovereignty between the UN member states, which often is considered to be closely related to the principle of non-intervention.[82] For there to be a substantial right of sovereignty for states, other states must have a correlating duty to respect that right and not intervene in the internal affairs of that state.[83] The principle of non-intervention is considered the corollary of the principle of sovereign equality of states.[84]

In addition to being part of customary international law, the principle of non-intervention has been included in several multilateral and bilateral treaties as well as other international documents. The principle of non-intervention is

[76] *(UK v Albania)* (Merits) [1949] ICJ Rep 4, 35.
[77] Christine Gray, *International law and the use of force* (3rd edn, Oxford University Press 2008) 75-76.
[78] Malcom Nathan Shaw, *International law* (8th edn, Cambridge University Press 2017) 62.
[79] *Nicaragua-case* (n 43) para 202.
[80] Shaw (n 78) 874.
[81] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI.
[82] Niki Aloupi, 'The Right to Non-intervention and Non-interference' (2015) 4 Cambridge J Int'l & Comp L 566, 569.
[83] R. J. Vincent, *Nonintervention and International Order* (Princeton University Press,1974) 14.
[84] *Nicaragua-case* (n 43) para 202.

found in Article 8 of the *Convention on Rights and Duties of States adopted by the Seventh International Conference of American States*[85] and the principle is also included in the *OAS Charter* and the OAU *Charter.*[86]

Between 1989 and 2001 the UNGA adopted nine resolutions condemning interference in electoral processes.[87] The UNGA resolution *Draft Declaration on Rights and Duties of States,*[88] includes a general provision in Article 3 according to which 'Every State has the duty to refrain from intervention in the internal or external affairs of any other State'. The resolution *Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral process*[89] regarding South Africa contains a similar provision. So does the *Declaration on the Inadmissibility of Intervention in the Domestic Affaires of States*[90] which in Article 1 state that 'No State has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal and external affairs of any other State.' The 1970 *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (Friendly Relations Declaration)*[91] also prohibits interventions.

A violation of the principle of non-intervention can also be a violation of the principle of non-use of force, if the intervention directly or indirectly includes the use of force.[92] A violation of the principle of non-use of force is, however, always a violation of the principle of non-intervention.[93]

The target of a prohibited intervention does not need to be state infrastructure, as private entities can also be the target of the interference if the operation aims to deprive the state authority of a matter within that state's *domaine réservé*.[94]

---

[85] *Convention on Rights and Duties of States adopted by the Seventh International Conference of American States* Montevideo 26 December 1933.
[86] Fisler Damrosch (n 23) 7.
[87] Jamnejad and Wood (n 72) 369.
[88] UNGA, *Draft Declaration on Rights and Duties of States*, 6 December 1949, A/RES/375.
[89] UNGA, *Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes*, 15 December 1989, A/RES/44/147.
[90] UNGA, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, 21 December 1965, A/RES/2131(XX).
[91] UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 24 October 1970, A/RES/2625(XXV).
[92] Shaw (n 78) 874.
[93] Jamnejad and Wood (n 72) 380.
[94] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 315-316.

3.2 The Two Elements

The principle of non-intervention consists of two elements. Firstly, there need to be an intervention and the intervention needs to be aimed at a matter in which each state is permitted to decide freely. Secondly, the intervention must be coercive.[95]

3.2.1 Matter in which Each State is Permitted to Decide Freely

The matters in which each state is permitted to decide freely, also known as *domaine réservé*, is neither static nor well defined but a dynamic concept.[96] The free determination of political, economic, cultural and social systems in addition to foreign policy and the exercise of permanent sovereignty of natural resources are included in the *domaine réservé* of states.[97] In the 1923 PCIJ advisory opinion *Nationality Decrees Issued in Tunis and Morocco* the court stated that the question of what is exclusive competence is relative and depends upon the development of international relations.[98] Both treaty law and the development of customary international law can result in a change of which matters that are included in the scope of the *domaine réservé*.[99] If a matter is regulated in international law (by treaties or customary international law) that matter is no longer within the *domaine réservé* of states. As a result of the increased globalisation and growing interdependence between states, the matters within the scope of states' *domaine réservé* decrease.[100] It is clear that a state's *domaine réservé* has limits, but where the limits are drawn is disputed and it is clear that the scope will evolve during time.[101]

One of the matters which is most clearly considered to be within the scope of the *domaine réservé* is the state's right to choose its political system and how the politics are organised. These matters constitute a central part of state sovereignty.[102] The hosting of democratic elections is in the centre of the

[95] Cf. *Nicaragua-case* (n 43) para 205.
[96] Nowak (n 135).
[97] Anders Henriksen, *International Law* (2nd edn Oxford University Press 2019) 258.
[98] *Décret de nationalité promulgués en Tunisie et au Maroc, avis consultative* (advisory opinion) 1923, C.P.J.I. séries B, No. 4, 28.
[99] Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' in Jens David Ohlin, Kevin Govern and Claire Finkelstein *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 264.
[100] Katharina Ziolkowski, 'General Principles of International Law as Applicable to Cyberspace' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publication 2013) 164.
[101] Ohlin (n 2) 1588; Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 314.
[102] Watts (n 99) 265.

domaine réservé.[103] The election process is left to the determination of each state and is mainly unregulated in international law.[104] National elections frequently lead to major shifts in a state's domestic and foreign policies. In some states a national competitive election could lead to a change of the regime or even a full-scale transition to democracy.[105] The elections affect a key democratic institution and the process by which the executive is peacefully replaced or retained and may therefore have great effect on the target state.[106] Actions which affect the result of an election in a state could therefore also greatly affect the state's political system and foreign policy.[107]

3.2.2 Coercion

To constitute a violation of the principle of non-intervention the act by the interfering state must be forcible, dictatorial or otherwise coercive in a way that deprive the target state of its control over the relevant matter.[108] The requirement of coercion therefore limits the principle's applicability.[109] Coercion includes acts that compromise the free will of the state and forces it to do or not do something against its will. The relevant aspect is the purpose, not the methods that are used to get the advantage. The means could be direct or indirect, physical or non-physical, military, economic, political or using cyberspace.[110]

Defining coercion as dictatorial interference is not accepted by all. Stanley Hoffmann claims that such a definition would make the principle to narrow and disapproves of defining intervention based on the type of activity. The purpose of the interfering state trying to make the target state do something which the target state otherwise would not do is presented as more relevant.[111]

Coercion has also been suggested to be seen as a spectrum. The spectrum ranges from minor interferences in another state's affairs at one end, to large-scaled military intervention at the other end. A clear line can, however, not

[103] Steven J Barela 'Cross Boarder Cyber Ops to Erode Legitimacy: An Act of Coercion' (Just security, 12 January 2017) <https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/> accessed 27 December 2019.
[104] Schmitt 'Virtual Disenfranchisement' (n 4) 49.
[105] Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 189.
[106] Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (n 21) 200.
[107] Kilovaty (n 6) 149.
[108] Oppenheim (n 73) 432ff.
[109] Jamnejad and Wood (n 72) 348.
[110] Cf. Watts (n 99) 269; Ohlin (n 2) 1592.
[111] Stanley Hoffman, 'The problem of intervention' in *Intervention in world politics* Hedley Bull (ed) (Clarendon Press 1986) 9-10.

be drawn between legal and illegal actions, since there are military interventions that can be legal and minor interferences in a state's affairs that may be illegal.[112]

The principle of non-intervention includes a right for states to freely choose its political system and formulate a foreign policy.[113] The most apparent and coercive form of political intervention is regime change, which can be done without force by supporting and funding insurrectionary opposition groups.[114] Such intervention is clearly a violation of the principle of non-intervention.[115]

Acts involving economic or political measures may constitute an intervention if such measures include the necessary coercive effect.[116] Such measures may be financial pressure or conditioning negotiations concerning admission into regional institutions to the acceptance of certain policies concerning secessionist attempts within a state.[117] Verbal declarations which aim at influencing another state can furthermore constitute a violation of the prohibition of non-intervention. That could be the case if a state's actions or declarations aim to affect the stability of a government, for example by encouraging secession, which could be considered coercive.[118]

Economic sanctions can also result in the target state changing its politics to be released of the sanctions. Economic sanctions are not, however, seen as a violation of the principle of non-intervention. In the *Nicaragua-case* the ICJ concluded that a total trade embargo is not a violation of international law which should indicate that less intrusive economic sanctions such as reducing export or import from a state do not violate the principle either.[119] The reason for this is the acts' lack of coercion. Economic sanctions should, however, be able to amount to coercion if the sovereign will of a state can be overborn by the imposition of the sanctions. That could be the case if a state is dependent on aid from primarily one state or mainly trades with that state. Vulnerable states' dependence on aid makes a withdrawal a very effective method of coercion.[120]

---

[112] Rosalyn Higgins, 'Intervention and international law' in *Intervention in world politics* Hedley Bull (ed) (Clarendon Press 1986) 30.
[113] *Nicaragua-case* (n 43) 205.
[114] Cf. *Nicaragua-case* (n 43).
[115] Jamnejad and Wood (n 72) 368.
[116] Oppenheim (n 73) 434.
[117] Marcelo Kohen, 'The principle of non-intervention 25 years after Nicaragua' (2012) 25 LJIL 157, 161.
[118] Aloupi (n 82) 576-577.
[119] Jamnejad and Wood (n 72) 370.
[120] Jamnejad and Wood (n 72) 370-371.

Whether it is a violation to simply fund non-insurrectionary political parties in another state is unclear.[121] Funding of a party given shortly before an election is presumably more effective and has a bigger chance of resulting in a change in government and is therefore more likely to be considered coercive and violate the principle of non-intervention than funding given at another point of time.[122] The states' practice of supporting parties in other states is becoming increasingly overt and is done without justification, which indicates that the states perceive such acts to be legal. The fact that the funding frequently is done through intermediates and that several states have created laws prohibiting foreign funding of political parties indicate the opposite.[123] If foreign funding of political parties is prohibited in the target state, such funding can be considered to be coercive. The same is true if the support is given to a party with coercive goals or the support is of such a magnitude that it becomes coercive.[124]

Acts such as granting or withholding recognition of another state's government, good office and various forms of cooperation does not constitute a violation of the prohibition of intervention since the acts are neither forcible nor dictatorial.[125] However, the question of recognising a state can according to some researchers constitute a violation of the principle of non-intervention under exceptional circumstances where the non-recognition is intended to force a change in policy.[126] Severing diplomatic relations, discontinuing exports or organising a boycott of products originating from the target state is neither generally considered a violation of the principle of non-intervention.[127] Such actions may at least indirectly be intended to persuade a state to pursue or discontinue a particular course of conduct, but does not constitute an intervention due to the lack of coercive aspects.[128] Persuasion, criticism and propaganda are also excluded from the definition.[129] There are, however, some who believe that propaganda can be a violation of the principle of non-intervention if the propaganda is false and it is intended to produce dissent or encourage insurgents. The circumstances in each case must be analysed.[130]

Requirements imposed on a state to comply with its international obligations within its territory, in order to negotiate a given issue, such as the requirement

[121] Jamnejad and Wood (n 72) 368.
[122] Jamnejad and Wood (n 72) 369.
[123] Jamnejad and Wood (n 72) 368.
[124] Jamnejad and Wood (n 72) 368.
[125] Oppenheim (n 73) 432ff.
[126] Jamnejad and Wood (n 72) 373.
[127] Oppenheim (n 73) 432ff.
[128] Oppenheim (n 73) 434.
[129] Henriksen (n 97) 258.
[130] Jamnejad and Wood (n 72) 374.

for a state to make its best efforts to collaborate with an international criminal tribunal as a condition for other states to alter their relations with the target state is not a violation of the principle of non-intervention due to the lack of coercion. Neither is the adoption of political positions regarding domestic situations, despite unfriendly language.[131] There is also a right for leaders of a state to engage in the political process of another state without violating the principle of non-intervention.[132]

The element of coercion is not satisfactorily defined, and it is unclear where the line is drawn between lawful political and economic pressure against a state and coercive intervention. Interventions which include force are always coercive but when no force is used, the determination becomes more complex.[133] There seem to be no consensus among states on a notion of coercion sufficient to amount to an intervention.[134]

3.3 Conclusions and Challenges

Regardless of a number of studies made, the exact nature, source and scope of the principle of non-intervention is still uncertain.[135] The vagueness of the definition of the principle of non-intervention enables the use of the principle to argue for opposing positions.[136] The vagueness of the principle is a longstanding issue and was almost 100 years ago described in the following, still very relevant, way:[137]

> *The subject of intervention is one of the vaguest branches of international law. We are told that intervention is a right; that it is a crime; that it is the rule; that it is the exception; that it is never permissible at all. A reader, after perusing Phillimore's chapter upon intervention, might close the book with the impression that intervention may be anything from a speech of Lord Palmerston's in the House of Commons to the partition of Poland.*[138]

[131] Kohen (n 117) 161.
[132] Ohlin (n 2) 1588.
[133] Aloupi (n 82) 576-577.
[134] Watts (n 99) 270; Kilovaty (n 6) 168.
[135] Jamnejad and Wood (n 72) 347; Christina Nowak, 'The changing law of non-intervention in civil wars – assessing the production of legality in state practice after 2011' (2018) 5 JUFIL 40.
[136] Nowak (n 135).
[137] Nowak (n 135).
[138] P H Winfield, 'The History of Intervention in International Law' (1922-1923) 3 Brit YB of Int'l L 130, 130.

An exact definition of the principle of non-intervention is probably not possible to create, due to the non-static nature of the principle. As pointed out in the *Nationality Decrees Issued in Tunis and Morocco* advisory opinion, the scope of the principle will evolve and naturally follow the development of other aspects of international law.[139] Hence, only a general definition of the principle can be made.

The principle of non-intervention constitutes of two elements, *domaine réservé* and coercion. The principle is violated if a state coercively interferes in another state's *domaine réservé*, matters which the target state is permitted to decide freely.

A state's *domaine réservé* includes a right for the state to freely decide the political, economic, cultural and social systems of the state in addition to foreign policy and the exercise of permanent sovereignty of natural resources. What is included in the free choice is determined by the scope of international law. The increasing globalisation and thereby increased number of areas regulated by international conventions and customary international law limit the scope of the *domaine réservé*. It is therefore impossible to create an exact definition of the scope of the *domaine réservé* of a state at a given point in time.

The element of coercion is, however, even further difficult to define. Coercion can be described as forcible, dictatorial or otherwise controlling acts or as acts that compromise the free will of the target state and forces it to do or not do something against its will. Despite the attempts to define coercion, the definition is still unclear and different interpretations are suggested.

The multilateral treaties, UNGA resolutions and existing case law including the principle of non-intervention were created in a different time and under different circumstances without the current technological possibilities in mind. The vagueness that exist regarding the application of the principle of non-intervention to traditional interference is increased regarding interference by means of cyberspace. Hence, the legality of electoral cyber interference aiming to manipulate voting behaviour is difficult to determine based on sources concerning the principle of non-intervention in general where the cyber aspect is not considered. The specific circumstances regarding violations of the principle of non-intervention resulting from cyber interference will therefore be examined in the following chapter.

[139] *Nationality Decrees Issued in Tunis and Morocco* (n 98) 28.

4 The Application of the Principle of Non-intervention to Electoral Cyber Interference Aiming to Manipulate Voting Behaviour

4.1 Non-intervention and Cyberspace

Cyber operations have, due to their anonymity, instantaneous cross-border effect and cost efficiency become a popular tool used by states in an effort to achieve strategic, political, economic and military objectives.[140] Regarding electoral interference, the internet has diversified the available means and methods to interfere.[141] Today many use the internet to receive their political information, join political campaigns, donate to political causes, sign petitions and some even vote online.[142] Hence, the effect of the internet in the political process is massive and states who wish to interfere in other states' elections have begun to take advantage of that.[143]

Electoral cyber interference effecting electoral infrastructure is generally considered a violation of the principle of non-intervention by many states.[144] Utilizing cyber operations to interfere in a state's ability to hold elections or manipulating the results of the election, is clearly coercive enough to constitute a violation of the principle of non-intervention.[145] However, the state opinion regarding electoral cyber interference aiming to manipulate voting behaviour is not as clear.[146]

The first criterion of the principle of non-intervention is that a matter within the scope of the *domaine réservé* should be affected. As concluded in the previous chapter, the political system of a state is one of the matters in which each state is permitted to decide freely. If voter manipulation affects the process of conducting an election or the outcome of an election it is an intervention into matters in which each state is permitted to decide freely.[147]

[140] Kilovaty (n 6) 150.
[141] Tsagourias (n 38).
[142] Moore (n 14) xii.
[143] Moore (n 14) xii.
[144] Tsagourias (n 38).
[145] Schmitt 'Virtual Disenfranchisement' (n 4) 50.
[146] Tsagourias (n 38).
[147] Barela (n 103); Schmitt 'Virtual Disenfranchisement' (n 4) 49.

The critical factor is therefore if electoral cyber interference aiming to manipulate voting behaviour can be defined as coercive. The criterion of coercion will, therefore, be analysed in the upcoming section. Firstly, different arguments regarding the definition of coercion will be categorised and analysed. Subsequently the categories of definitions will be applied to the hypothetical case from chapter 2.2.

4.2 The Element of Coercion Regarding Attempts to Affect Voting Behaviour by Electoral Cyber Interference

The requirement of coercion applies to all forms of non-intervention alike and is therefore required for voter manipulation to amount to a violation of the principle of non-intervention.[148] A variety of different approaches to defining the criterion of coercion in the context of cyber voter manipulation have been presented in the legal literature. As an effect of the differences of the definitions, the opinions regarding whether voter manipulation can amount to coercion and thereby a violation of the principle of non-intervention are conflicting.[149]

Despite comprehensive differences between the definitions of coercion, similarities can be found. The definitions can be divided into two main categories which both focus on coercion as the lack of freedom of choice, but in different ways. In the first category, coercion is defined as a lack of freedom of choice due to a state being forced to act in a certain way because of impending consequences. The first category will hereafter be termed 'forcible coercion threatening of consequences'. The second category define coercion as a lack of freedom of choice due to the fact that the opinions of the voters regarding the election were formed in a manipulated environment. The second category will subsequently be termed 'coercion manipulating the voters' opinion forming environment'. Within each category of definitions of coercion, there are several different definitions, but the definitions within the same category can be said to have the same approach to defining coercion. The definitions of coercion in the first category can be described as more palpable than the second, more metaphysical one.

A question relevant for both categories of definitions of coercion is how direct the causal nexus must be between the cyber operation performed by the

[148] Ohlin (n 2) 1589.
[149] Kilovaty (n 6) 167.

interfering state and the election results in the target state.[150] A majority of the experts behind the Tallinn Manual argued that indirect causality can constitute coercion, which was disputed by a minority.[151] Only if indirect causality is sufficient, can voter manipulation constitute an intervention, since the cyber operations only indirectly affect the election results by affecting the voters choice of candidate.[152] Such a situation could be comparable with the support given by the United States to the Contras in Nicaragua. The coercion in that case was also indirect since the United States simply supported the Contras, who performed the actual coercive acts. In the case, the court stated that indirect intervention can violate the principle of non-intervention.[153] Some scholars have, however, argued that indirect coercion makes it less likely, but not impossible, for the criterion of coercion to be fulfilled.[154]

Another question equally relevant for both of the two categories of definitions of coercion is whether it is the intent of the coercive act or the result it achieves that is determining. It has been argued that the actual outcome of the interference must not be the one imagined by the interfering state. It is enough that the interfering state intended their act to be coercive to constitute a violation of the principle of non-intervention. Furthermore, simply threatening to conduct a coercive act can amount to coercion if the threat is made to compel the target state to act in a certain way.[155] It has also been argued that it is the effect or consequences of an action, and not the intent of the intervening state, that is decisive in the assessment of whether an action constitute a prohibited intervention. This reasoning has the effect that a state which supports a group of hackers in another state (for example based on common ideology or religion) could be violating the principle of non-intervention if the hacker group use the support to coerce the target state.[156] The effect or consequence, even if it is only collateral, would be enough. The crucial element is that the support of one state results in the limitation of the target state's sovereignty.[157]

Nevertheless, these conclusions are not conflicting. The fact that the intent, without a measurable result, by a state to intervene in another state constitutes coercion, does not exclude effective intervention without the intent to intervene from being coercive, and vice versa. It simply shows that either

[150] Schmitt 'Virtual Disenfranchisement' (n 4) 51.
[151] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 320.
[152] Schmitt 'Virtual Disenfranchisement' (n 4) 51-52.
[153] Cf. *Nicaragua-case* (n 43) especially para 205.
[154] Schmitt 'Virtual Disenfranchisement' (n 4) 151-152 f.
[155] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 322-323; Schmitt 'Virtual Disenfranchisement' (n 4) 52.
[156] Watts (n 99) 269; Cf. *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Merits) [2005] ICJ Rep 168, para 163.
[157] Watts (n 99) 269.

intent or result is sufficient to be coercive which widens the definition of coercion and consequently the scope of the principle of non-intervention.

4.2.1 Forcible Coercion Threatening of Consequences

The experts of the Tallinn Manual[158] defines coercion as 'An affirmative act designed to deprive another State of its freedom of choice, that is, to force the State to act in an involuntary manner or involuntarily refrain from acting in a particular way'.[159] Watts has defined the criterion of coercion as an intervention where the intervened state cannot terminate the intervention at its pleasure.[160] According to Ohlin, coercion should have the structure of: do or don't do this or there will be a specific consequence. The target state follows the direction of the interfering state as a result of the looming consequences being intolerable.[161] Hence, to constitute coercion, a target must be forced, the target must be forced to do or not do something and the target must be threatened with a consequence. [162]

According to Ohlin, basing his conclusion on the *Nicaragua-case,* even though this was never explicitly stated in the judgement, the impending consequence forcing the target state to act in a certain way must be an illegal act. If the impending consequence is legal according to international law, the threat from the intervening state is simply a strategic behaviour and not coercion.[163]

Nevertheless, all experts do not agree with this interpretation of the *Nicaragua-case*.[164] Some scholars claim that an act can constitute a violation of the principle of non-intervention, regardless of whether the act is illegal or not. The relevant aspect is that the act forces the target state to act in a certain

[158] The view presented in the first edition of the Tallinn Manual, was that the manipulation of the public opinion on the eve of an election by for example altering online news services in favor of a specific party, spreading fake news of a specific party or online services being shut down, could amount to a violation of the principle of non-intervention. The scope of the first edition of the manual was however mainly *jus ad bellum* and *jus in bello* and cyber operations below the level of use of force was sparsely mentioned. In the second more broadened edition, the same statement was not made. The lack of a similar provision in the second edition indicates that electoral interference manipulating voting behavior is not considered coercive. (Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 4, 45; Schmitt and Vihul, *Tallinn manual 2.0* (n 46).)
[159] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 317.
[160] Watts (n 99) 256.
[161] Ohlin (n 2) 1589.
[162] Ohlin (n 2) 1592.
[163] Ohlin (n 2) 1589.
[164] Ohlin (n 2) 1589.

way.[165] By support from philosophical literature it can also be argued that not only threats, but also offers which come with conditions may be coercive, if the offer is too good to refuse.[166]

The purpose of the principle of non-intervention is to protect every states' sovereignty and the right to choose freely in certain matters. Threats of legal as well as illegal consequences can limit the possibility of a state to make a truly free choice. An example is the threat of a state, being the main contributor of aid to a state in crisis, to withdraw its support. Therefore, in my opinion, the legality of the coercive act should not be determining whether an act prevents the target state from making a free decision. Such an interpretation of the *Nicaragua-case* would vastly limit the scope of acts defined as coercive.

There are divergent opinions regarding whether a state can be coerced unknowingly. Most experts behind the Tallinn Manual argued that an act can amount to coercion despite not being known by the target state. Being aware of being coerced is therefore not a precondition for being a victim of an intervention.[167] Some experts conversely argued that the fact that an electoral intervention is covert prevent it from being coercive, the target state needs to know of the pressure to be coerced to act in a certain way.[168]

For a state to be compelled to act in a certain way to avoid the impending consequences, the state needs, according to me, to be somewhat aware of what the consequences are and what to do to avoid them. Lacking such knowledge, the target state will have no incentive nor possibility to act according to the will of the interfering state. If a state unknowingly could be coerced, the scope of which actions that could amount to coercion would be much widened.

According to some, electoral cyber interference aiming to manipulate voting behaviour must coerce a specific target and the target must be compelled to act or refrain from acting in a certain way to avoid specific consequences. According to Ohlin and Duncan Hollis, it is questionable if voter manipulation fits that definition.[169] According to Ohlin, the target could either be the voters or the disfavoured candidate in the campaign. The compelled act could be to vote for another candidate than the voters would have done without the coercion or the disfavoured candidate being forced to adopt a more favourable policy towards the interfering state. The threatened

[165] Ohlin (n 2) 1592-1593.
[166] Ohlin (n 2) 1589-1590.
[167] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 320-321.
[168] Kilovaty (n 6) 167.
[169] Ohlin (n 2) 1592; Duncan Hollis, 'The Influence of War; the War for Influence' (2018) 32 Temp Int'l & Comp LJ 31, 41.

consequences might be to withhold benefits if the 'wrong' candidate won or to be more cooperative if the preferred candidate won.[170] However, Ohlin questions whether a threat or offer would be made, either explicitly or implicitly, and also if the voters of a state can be equated with the state.[171]

According to me, this quite technical analysis of Ohlin may create problems that do not really exist. The conclusion that the disfavoured candidate or the voters would be the target of the interference overlooks the fact that intervention can be indirect. The target is the state that is forced to act in a certain way it would not have without the interference, electing a candidate that otherwise would not be elected.

However, in my opinion, the question is if the target state truly was forced and what the impending consequences were. When cyberspace is used to manipulate the voters, the core of the method is to do it covertly. The threat of consequences could perhaps be done without referring to the influence campaign, by simply stating what effect the election of the disfavoured candidate would imply for the relations of the target and interfering state. Scenarios where explicit or implicit threats of consequences are made, result in questionable causality. With threats of consequences, it would most likely be the threat and not the influence campaign that compels the voters to vote for the interfering state's preferred candidate. This is the core of the problem. The objective with manipulating the voters is to affect their opinion, to make them prefer or disapprove of a certain candidate. Having a candidate being chosen due to impending, unbearable consequences otherwise being imposed, does not entail the opinion of the voters being manipulated and is therefore not interference by voter manipulation. If the opinions are manipulated, the consequences are not the reason for the preferred candidate being elected. Hence, the threat of consequences and the altering of voter opinions must be considered irreconcilable.

This conclusion is in line with the one of the experts of the Tallinn Manual. Applying their definition of coercion, the experts conclude that persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness and other similar actions are not coercive and therefore not a violation of the principle of non-intervention. Neither are espionage nor diplomacy and diplomatic processes.[172] According to the Tallinn Manual, a state-sponsored public information campaign promoting a certain political decision in the target state is not a violation of the principle of non-intervention due to the lack of the key element of compelling the target state to act in a certain way.

[170] Ohlin (n 2) 1592.
[171] Ohlin (n 2) 1592.
[172] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 318-319, 323.

Such acts simply influence voluntary actions of the target state and do not coerce the state to act in a certain way.[173] Some experts nevertheless argue that acts that normally would not amount to coercion could reach that threshold due to the specific consequences and context. Therefore, it is impossible to conclude that some acts can never be coercive.[174] This disclaimer can always be made, considering that it is impossible to predict all possible scenarios. However, the fact does remain. The influence campaign influences the opinion of the voters, making them want to vote for a specific candidate. Threats of consequences force the voters and thereby the state to act in a certain way in fear of unbearable consequences.

4.2.2 Coercion Manipulating the Voters' Opinion Forming Environment

One of the supporters of the second category of definitions of coercion, Nicholas Tsagourias, argues that a state's will is only free if the sourcing of it is also free. The conclusion is based on the relationship between the principle of non-intervention and that of self-determination. The principle of non-intervention protects the principle of self-determination and in the latter, it is included a right for the people to really and freely choose their political system. The process of forming a free will is therefore also protected by the principle of non-intervention according to Tsagourias.[175]

Analysing the definition of the criterion of coercion, Tsagourias emphasizes Oppenheim's definition of coercion as deprivation of control of a matter but disregard the other part of Oppenheim's definition, dictatorial or forcible coercion. When a foreign state manipulates the will and authority of another state at its source, in the process of its formation, that is coercion by the meaning of control. By affecting the will of the voters by manipulating the environment in which the opinion of the voters are formed, the interfering state controls the choices made by the voters, which by extension means that the interfering state controls the authority and will of the elected government.[176]

Similarly, Björnstjern Baade describes voter manipulation as coercive in the sense of a manipulation of the voters' capacity to reason. Mainly focusing on disinformation and fake news, Baade argues that it is coercion when false information is introduced since the facts are distorted. The presented 'facts'

[173] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 318-319.
[174] Schmitt and Vihul, *Tallinn manual 2.0* (n 46) 318-319.
[175] Tsagourias (n 38).
[176] Tsagourias (n 38).

create an environment that constrains the voters' freedom of choice by the false facts making some options no longer seem viable and other mandatory.[177]

Russel Buchan suggests a definition of coercion that primarily protects the metaphysical aspects of sovereignty, the political integrity of the state and not only the physical aspect of sovereignty. According to Buchan, all 'Conduct which compromises or undermines the authority of the state should be regarded as coercive'. Such a more inclusive definition of coercion is required to protect every matter included in state sovereignty.[178]

The relatively narrow definition of the criterion of coercion in the *Nicaragua-case* does not limit a broader definition of coercion according to Buchan. The definition of coercion in the case should not be applied to the principle of non-intervention in general, when being applied to acts not including force. It is clearly stated in the case that the court only considered the aspect of non-intervention that was relevant to the case.[179] This conclusion is supported by Patrick Terry. The United States' support to the Contras in the *Nicaragua-case* was large-scaled and aimed at overthrowing a government by force, which resulted in there not being any need for the court to elaborate on the element of coercion regarding more low-intensity interventions.[180] Case law is also, according to Article 38(1) of the ICJ Statute, only a subsidiary source of international law. Therefore, there is nothing in the case that prevents another interpretation of coercion being applicable to more low-intensity intervention.[181]

Barrie Sander argues that some support of the definition of coercion as manipulation of the voters' opinion forming environment can be found in the 1970 *Friendly Relations Declaration* according to which all states have the right to choose its political system, 'without interference in any form'.[182]

The fact that the interference by voter manipulation is done covertly, for example by troll-farms, does according to Schmitt in fact deprive the voters of a free choice by creating a situation where the voters cannot objectively evaluate the existing information. Since the voters are not aware of the

[177] Björnstjern Baade, 'Fake news and international law'(2018) 29 ELIJ 1357, 1363-1364.
[178] Russel Buchan, 'The International Legal Regulation of State Sponsored Cyber Espionage' Anna-Maria Osula and Henry Rõigas (eds) *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016) 78.
[179] *Nicaragua-case* (n 43) para 205; Buchan (n 178) 79.
[180] Patrick C R Terry, 'Don't Do as I Do - The US Response to Russian and Chinese Cyber Espionage and Public International Law' (2018) 19 German LJ 613, 620.
[181] Buchan (n 178) 79; Terry (n 180) 620.
[182] Barrie Sanders 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 CJIL 1, 23.

manipulation of their decision-making, their control of their government is weakened and distorted. The concealed nature of the origin of the trolling distinguishes it from mere influence.[183] Similarly, Baade argues that covert interference by spreading disinformation deprives the voters of the possibility to assess the information's trustworthiness, which is an indication of coercion.[184] The hacking and releasing of information instead have the effect of tainting the electoral process and is an illegal act in many countries. The electorate's freedom of choice is in this way negatively affected.[185]

Applying a definition of coercion, whereby coercion is the manipulation of the voters' opinion forming environment, resulting in the voters not freely electing their preferred candidate, will according to me create a stronger protection of the essence of independence and sovereignty, the truly free choice. When the opinion of the voters is manipulated and they no longer freely choose their candidate, the authority structure is undermined.

In the present globally interdependent society, choices are generally, more or less consciously, influenced by the will of other states. This definition of coercion as manipulation of the voters' opinion forming environment risk creating a very wide scope of the principle of non-intervention where most states which have stakes in the outcome of another state's election risk violating the principle of non-intervention. A relevant question is also if it should be enough that there have been influence operations to determine that the voters did not make a free choice, or if there needs to be evidence of the influence actually affecting the votes or even affecting the results of the election.

According to Steven J. Barela, the spreading of fake news might not in itself reach the criterion of coercion. Nevertheless, the spread of several misleading stories to millions of the public can, if seen in the context of other efforts to influence the election, be a part of fulfilling the criterion of coercion.[186] Similarly, Tsagourias emphasize that a certain degree of severity is needed for an influence operation to be coercive.[187] Buchan also concludes that not all acts interfering with the authority structure of a state should amount to coercion. Interference that simply irritate or is inconvenient does not amount to coercion.[188]

[183] Schmitt 'Virtual Disenfranchisement' (n 4) 51.
[184] Baade (n 177) 1364.
[185] Schmitt 'Virtual Disenfranchisement' (n 4) 51.
[186] Barela (n 103).
[187] Tsagourias (n 38).
[188] Buchan (n 178) 80-81.

According to Tsagourias, the decisive element is that the influence operation was performed by manipulating and misleading means purposively designed to exert control over the choice of politics in the target state.[189] This is in line with Barela's arguing that it is more probable that the spreading of false information, compared to true but confidential information, is coercive. When the information also is released in different stages and in different media outlets to create the biggest impact, the voter manipulation is more likely to amount to coercion.[190]

Schmitt is an advocate of measuring severity based on effect and consider an act coercive if the outcome of the election actually is affected by the voter manipulation.[191] The interfering state's manipulation has subordinated the will of the target state if the 'wrong' candidate wins, if a strong candidate's support is weakened or if a weak candidate's support is strengthened.[192] This does, however, go against the general opinion that intent, despite lack of result, is enough to constitute coercion.

Even though the exact definition of coercion is perceived differently, the definitions have in common that all influence operations do not amount to coercion. The definition can be limited by requiring a certain degree of severity, by the operation needing to constitute of manipulating and misleading means or by interference needing to be part of a larger operation and not only isolated events. In my opinion, having these kinds of limitations avoid the issue of creating a very wide scope of intervention where it is hard to avoid intervening in other states' internal affairs. Drawing the limit between the spread of false and true information would be unfortunate since true but confidential information spread at strategic points in time, regarding a specific candidate can be as effective as using fake information to manipulate the opinions of the voters. Accurate information should, however, generally not be considered coercive since it is important for the voters to be well informed (despite the nationality of the informant), but the context of the spread of information must be taken into account, as stated by Barela.[193]

Exactly where to draw the limit regarding interference coercive enough to constitute a violation of the principle of non-intervention will most likely have to be determined from case to case. The question of whether the magnitude of the operation or the effect of the operation, the votes, should be the determining factor when measuring the severity remains.

---

[189] Tsagourias (n 38).
[190] Cf. Barela (n 103).
[191] Schmitt 'Virtual Disenfranchisement' (n 4) 50.
[192] Schmitt 'Virtual Disenfranchisement' (n 4) 51.
[193] Barela (n 103).

This second category of definitions of coercion has been challenged by Hollis, who questions if electoral cyber interference aiming to manipulate voting behaviour could amount to a violation of the principle of non-intervention. The fact that the aim of the influence operations are to change the opinion of the voters in the target state contradicts the existence of coercion.[194] The aim of the interference is, as Hollis notices, to change the opinion of the voters, but since the basis of the second category of definitions of coercion is that the opinion of the voters were affected by being created in a manipulated environment, the objection has little validity in this context.

4.2.3 Concluding Summary

Forcible coercion threatening of consequences, the first category of definitions of the criterion of coercion, focuses on the target state being forced to involuntarily act in a certain way, not being able to stop the coercive act, and not acting in that way would result in consequences that the target state perceives as unacceptable. According to this category of interpretations of the criteria of coercion, voter manipulation does not amount to coercion, since the aim is to influence the voters' opinion and not forcing them to vote in a certain way.

Coercion manipulating the voters' opinion forming environment, the second category of definitions of the criterion of coercion, focuses on the interfering state manipulating the political environment where the voters form their opinion and chose which candidate to vote for. There is no tangible compulsion which force the voters to vote for a specific candidate, the voters vote for their preferred candidate. However, the candidate that they believe they prefer is an effect of the interfering state having manipulated the political environment. The interfering state therefore coerce the target state by controlling the voters. According to this category of interpretations of the criterion of coercion, voter manipulations is coercive due to it manipulating the political environment where the opinions of the voters are formed.

There is a fundamental difference between the two categories of definitions of the criterion of coercion. The first category contains definitions according to which the voters' choice of who to vote for is free. The influence simply affects their free opinion, but the voters still have the option to vote for whoever they prefer, without fearing for consequences, their opinion is still free. The second category contains definitions according to which the

[194] Hollis (n 169) 41.

manipulated political environment forces the voters to vote for a specific candidate. The voters might have a theoretical possibility to vote for another candidate, but in reality, the interfering state control who the voters vote for and the voters no longer have a free opinion or a free choice. The difference is how the voters' opinion is being perceived, as free or not free.

4.3 Criteria or a Holistic Approach?

There are different suggestions regarding how to evaluate if a state's voter manipulation amount to either of the two different categories of definitions of coercion. Some suggest sets of criteria, while other advocate for a more holistic approach or a combination of both.

Hollis has suggested the application of five criteria to determine the legality of influence operations (making no difference between different forms of influence operations); transparency, extent of deception, purpose, scale and effect. The element of transparency distinguishes between operations where the state is open about the origin of the actions and operations where the state tries to hide the origin of the actions. Deception distinguishes between emanating false (for example fake news) or true information (for example hack-and-leak operations). The element of purpose distinguishes between operations which aim to change the public opinion in general and operations which intend to change their views on specific matters or operations which simply aim to create chaos. The scale of the operations is also a determining factor. Lastly, the effect of the operation considers how serious the effect resulting from the influence operation is.[195]

Several scholars suggest the application of the three dimensions of consequentiality created by Myres S. McDougal and Florentino P. Feliciano.[196] McDougal and Feliciano suggest three dimensions of consequentiality (though created in another context) being considered to determine if the criterion of coercion is fulfilled. These dimensions are 'The importance and number of values affected, the extent to which such values are affected and the number of participants whose values are so affected'.[197] Applying McDougal's and Feliciano's criteria on electoral cyber interference, the nature of the target state's interests which are affected by the operations, the scale of the effects in the target state and how many actors that are affected by the operation should be considered to determine if the interference is

[195] Hollis (n 169) 36-38.
[196] Watts (n 99) 257; Buchan (n 178) 80-81; Kilovaty (n 6) 169.
[197] Myres S McDougal and Florentino P. Feliciano, 'International Coercion and World Public Order: The General Principles of the Law of War' (1958) 67 Yale LJ 771, 782.

coercive enough to amount to a violation of the principle of non-intervention.[198] Tsagourias suggests that the number of actors affected could be estimated by, for example the number of people that have seen a video containing disinformation.[199] It is emphasized that despite applying the three criteria, it is still complicated to determine whether an act is coercive or not.[200] It can be noticed that advocates for the first as well as the second category of definitions of coercion suggest the use of McDougal and Feliciano's criteria.[201]

The application of criteria to evaluate the coerciveness of an act has been opposed by some. According to Buchan, the facts in each case of cyber operations must be considered to assess to what extent the target state's sovereignty was compromised and the scale of the operation.[202] Ohlin argues that the assessment of whether or not interference constitutes an illegal intervention should be determined holistically based on all facts regarding the situation and not based on certain formalistic and abstract requirements. Ohlin also suggests that the criterion of coercion should be assessed based on the scale of the effect of the overall interference.[203] Watts oppositely argues that the merits of the use of McDougal's and Feliciano's criteria is to not only base the assessment of coercion on the level of interference and intrusion but to include all relevant factors.[204]

The choice between the application of criteria or a more holistic approach is, according to me, somewhat misleading. Choosing one does not exclude the other. While criteria can facilitate to observe a number of relevant aspects of coercion, there is always a risk that an aspect relevant in the specific case, but not in interference in general, is overlooked. A holistic approach can be better adapted to the specific circumstances in the case. However, the use of criteria can result in more equivalent assessments since the interference is assessed based on the same premises. An assessment based on criteria but with a concluding holistic assessment could be beneficial.

Which of the sets of criteria suggested that would be most useful and which set that is more or less inclusive is difficult to determine without applying them to an actual case. This will therefore be further analysed in the following section.

[198] Watts (n 99) 257.
[199] Tsagourias (n 38).
[200] Kilovaty (n 6) 169.
[201] Watts (n 99) 257; Buchan (n 178) 80-81; Kilovaty (n 6) 169.
[202] Buchan (n 178) 80-81.
[203] Ohlin (n 2) 1593.
[204] Watts (n 99) 257.

4.4 The Different Approaches Applied to the Hypothetical Case

Both the above presented sets of criteria and a holistic approach can be used to evaluate whether acts of states are coercive when applying either of the two categories of definitions of the criterion of coercion. The outcome depends on the category of the definitions of coercion. To illustrate the outcome of the application of the approaches to the two different categories of definitions of coercion, the hypothetical case from section 2.2 will be used.

4.4.1 Forcible Coercion Threatening of Consequences

4.4.1.1 Using Criteria

Applying Hollis' five criteria,[205] State B's voter manipulation should be measured based on transparency, extent of deception, purpose, scale and effect. The criteria focus on facts in the case and the specific definition of coercion does therefore not affect the outcome of the evaluation. There is a clear lack of transparency by State B's use of identity falsification, posing as citizens of State A and concealing the origin of advertisement and hack-and-leak operations. The interference consists of both true information from hack-and-leak operations, but also false information such as disinformation and the true and false information was purposely intermingled to increase the deception of the voters of State A. The aim of the interference was to change the opinion of the public in State A on a specific question, to perceive candidate X as the most suitable leader and to vote for candidate X. The scale of State B's voter manipulation is to be considered relatively large-scaled using several different methods, different targets (government and private) as well as using different forums such as social media and other websites. Regarding the effect, it has not been proven that the interference actually affected the opinion of the voters or had an effect on the outcome of the election in State A. It can therefore not be concluded that the voter manipulation had any effect. The lack of proven effect results in State B's interference not fulfilling all the criteria and the interference cannot be considered coercive and a violation of the principle of non-intervention.

Applying the three criteria from McDougal and Feliciano's consequentiality theory, State B's interference is evaluated based on 'The importance and number of values affected, the extent to which such values are affected and

[205] Hollis (n 169) 36-38.

the number of participants whose values are so affected'.[206] Here the specific definition of coercion as forcible coercion threatening of consequences will have an effect on the outcome of the assessment.

The values that could have been affected by State B's interference in the electoral process are State A's right to freely choose its political leader which is included in State A's sovereignty. The complicated question is to which extent, if at all, the values were affected. It cannot be proven that the interference of State B was the reason that candidate X was elected. Even if that would have been the case, the definition of coercion as forcible coercion threatening of consequences makes the interference of State B impossible to have affected the values of sovereignty. As the interference of State B simply is perceived as influencing the free will of the voters, not forcing them to vote for candidate X, they retained their free choice and the sovereignty was not affected. Since the interference did not affect any values, there were also no people who had their values affected. Defining coercion as forcible coercion threatening of consequences therefore excludes State B's interference from being coercive and thereby from being a violation of the principle of non-intervention.

4.4.1.2 Using a Holistic or Combined Approach

A completely holistic approach with a case to case determination can also be used. The definition of the criterion of coercion has a great effect on the outcome of the holistic approach. To constitute coercion the voter manipulation of State B needs to force State A to elect candidate X. State A must not be able to stop the voter influence at its own pleasure and if candidate X is not elected, there will be consequences.

Many of the methods used by State B to interfere in State A are legal (though differences between states may occur). According to some interpretations of the *Nicaragua-case*, this would exclude State B's interference from constituting coercion. However, following the conclusion above,[207] illegality is most likely not a prerequisite.

The interference performed in State A is covert since identity falsification is used and State B tries to conceal the origin of the influence operation. The voters of State A are therefore not aware of being coerced. Following the line of reasoning above,[208] State A's lack of knowledge of the operation should prevent State B's interference from being coercive. However, applying the

[206] McDougal and Feliciano (n 197) 782.
[207] See ch 4.2.1., 33.
[208] See ch 4.2.1., 36.

reasoning of the Tallinn Manual, knowledge is not required. The fact that State B is accused of being the perpetrator could also be interpreted as State A being aware of the coercion, fulfilling the alleged requirement of knowledge.

The target of State B's interference is clearly State A, since the influence is aimed at the election and thereby the political control of state A. State B aims to force State A to choose candidate X or at least to strengthen the support of candidate X and undermine the support of candidate Y. The election of candidate X indicates that the aim was achieved, it is, however, not apparent if the interference had any real effect, or if candidate X would have won without the support. However, that is not important, since either the intent or the result is enough to constitute coercion. The aim is achieved by indirect causation, by affecting the voters who subsequently affect the outcome of the election. The indirect causality might lessen the probability of the interference being coercive, but it is still possible.

Hence, the remaining question is the threat of consequences. According to this definition of coercion, State A should comply and elect candidate X because of the consequences another decision might result in. The electoral interference of State B is covert, and when interference is suspected, State B denies the allegations. During those circumstances it is difficult for State B to even implicitly threaten (or bribe) with consequences. Even if State B in another context would indicate its approval of candidate X, which might indicate consequences if candidate Y would be elected, the coercive interference in the election process would then be the implicit threat of consequences. The possible effect on the election result in State A would be a result of the implicit threat, not the interference campaign of State B. There is therefore a lack of causality and when coercion is defined as forcible coercion threatening of consequences the holistic approach results in State B's interference not being a coercion and thereby not a violation of the principle of non-intervention.

Since both sets of criteria as well as a holistic approach results in State B's interference not being coercive when coercion is defined as forcible coercion threatening of consequences, a combination will have the same result. State B's interference was not a violation of the principle of non-intervention.

4.4.2 Coercion Manipulating the Voters' Opinion Forming Environment

4.4.2.1 Using Criteria

The application of Hollis' five criteria (transparency, extent of deception, purpose, scale and effect)[209] will lead to the same result as if coercion is defined as forcible coercion threatening of consequences. The outcome will be the same due to the fact that the five criteria only analyse the facts in the case and not the interpretation of coercion. Consequently, according to Hollis' criteria, State B's influence campaign does not constitute a violation of the principle of coercion when coercion is defined as manipulating the voters' opinion forming environment either.

The application of the three criteria of McDougal and Feliciano[210] is, however, affected by the definition of the criterion of coercion. The values that could be affected are still State A's right to freely choose its political leader which is included in State A's sovereignty. Furthermore, regarding coercion defined as manipulating the voters' opinion forming environment, the question is to which extent the values were affected, that is decisive. As stated above, the effect of State B's interference in electing candidate X has not been proven. However, if it could be proven that candidate X was elected as a result of State B's interference, the sovereignty would have been extensively affected. The coercion of State B is here defined as manipulating the voters' opinion forming environment and the manipulation of the opinion of the voters is considered coercion. The voter manipulation deprived the voters of their free will and thereby forced candidate X to be elected. State B determining the political leader of State A is a sever restriction of State A's sovereignty. If the election of candidate X could be proven to be a result of State B's interference, the entire population of State A would have been affected by the restriction of the sovereignty. The fact in the case is, however, that the effect of the interference cannot be proven. Therefore, the interference cannot be proven to be coercive, despite coercion being defined as manipulating the voters' opinion forming environment, and State B's voter manipulation does not violate the principle of non-intervention.

4.4.2.2 Using a Holistic or Combined Approach

As mentioned above[211], the definition of the criterion of coercion has a great effect on the outcome of the holistic approach. According to the second

[209] Hollis (n 169) 36-38.
[210] McDougal and Feliciano (n 197) 782.
[211] See ch. 4.4.1.2., 44.

category of definitions of coercion, State A was coerced if the opinion of the voters in State A was affected by State B's manipulation of the environment in which the opinions of the voters were formed. The opinions being formed in a manipulated environment consequently results in State B controlling and manipulating the authority of State A. Due to State B's relatively extensive campaign it is apparent that the opinions of the voters in State A were formed in a manipulated environment. It is also possible, but not necessary, that the opinions of the voters in State A was affected by State B's manipulation. This is, however, not relevant since both intent and effect can be enough to amount to coercion.

However, the interference must reach a certain level of severity to constitute coercion according to the definition of coercion as manipulating the voters' opinion forming environment. State B used many different methods of interference such as hack-and-leak operations, propaganda, disinformation, sentiment amplification, identity falsification, imitating citizens of State A and DDoS-attacks on websites. Both parties and government institutions in State A was targeted. The methods were both manipulating, by strongly emphasizing the merits of candidate X and discrediting candidate Y and adapting the message to different groups of voters, but also misleading by including a few false documents among the large leaks of confidential but accurate material and by the spread of disinformation and hacking and posting false statement imitating candidate Y. Different forums were also used, such as social media, party websites and comment sections of newspaper. The scalability was increased by State B not only using paid trolls but also automatic bots. Regardless of which criterion that is used to exclude minor interference from the definition of coercion (certain methods of voter manipulation, only misleading acts, a certain severity) the interference of State B is most likely to amount to that level.

Hence, applying a holistic approach to the second category of definitions of coercion, results in State B's voter manipulation amounting to coercion and thereby constituting a violation of the principle of non-intervention.

It is unclear what a combination of the application of criteria and a holistic approach would result in regarding coercion defined as manipulating the voters' opinion forming environment. According to the sets of criteria, State B's interference was not coercive. According to a holistic approach the interference was coercive. The intent of combining either set of criteria with a holistic approach is to make sure that aspects relevant in the specific case that do not fit any specific criterion is not overlooked. In the case of State B's voter manipulation there are no specific aspects that are not considered within the sets of criteria. The holistic approach should therefore not change the

outcome of the application of criteria when using a combined approach. The interference of State B's does therefore not constitute coercion when evaluated based on a combination of criteria and a holistic approach and does therefore not amount to a violation of the principle of non-intervention.

4.5 Concluding Summary

Hollis' criteria simply analyse the facts of the interference and the definition of the criterion of coercion is therefore not relevant. Irrespective of the definition of coercion, Hollis' criteria of effect cannot be proven to be fulfilled due to the fact that the interference's effect on the outcome of the election has not been proven. Consequently, according to this approach, the voter manipulation of State B does not constitute a violation of the principle of non-intervention.

When applying the criteria of McDougal and Feliciano, the definition of coercion affects the result. Defining coercion as forcible coercion threatening of consequences, the value of sovereignty cannot be affected. The voter manipulation of State B is perceived as simply influencing the voters, not forcing them to vote for a specific candidate. The choice of the voters is still considered free. Therefore, State B's interference cannot be coercive and thereby not a violation of the principle of non-intervention. Defining coercion as manipulating the voters' opinion forming environment, the values of sovereignty can be affected. By manipulating the environment in which the voters of State A formulate their opinions, the choice of the voters is no longer free but controlled by the interfering state, State B. The actual effect of the interference has, however, not been proven. The lack of evidence of the effects on the values therefore exclude State B's interference from this definition of coercion as well. State B's interference is, thereby, not a violation of the principle of non-intervention based on either of the definitions of coercion, but for different reasons.

When applying a holistic approach, defining coercion as the lack of freedom of choice due to a state being forced to act in a certain way to avoid impending consequences, results in State B's voting manipulation not constituting a violation of the principle of non-intervention. Forcible coercion threatening with consequences require State A to be forced to follow State B's direction in fear of impending consequences. Aiming to influence the opinion of the voters in State A aims to actually change the opinion of the voters (though on false premises) and make them want to vote for candidate X. Voting out of fear of impending consequences and voting for the preferred candidate are two different motivations. If the voters vote for candidate X out of fear of

consequences (which this definition of coercion requires), it is not the manipulation but the threat that has made them do so. Voter manipulation can therefore never be coercion in the definition of forcible coercion threatening with consequences.

Defining coercion as the lack of freedom of choice due to the manipulation of the voters' opinion forming environment, results in voting manipulation violating the principle of non-intervention, if the voter manipulation reaches a certain level of severity. When the environment in which the voters of State A formulate their opinion is manipulated, their choice is no longer free but controlled by State B. State A is therefore coerced to elect a specific candidate, which is a violation of the principle of non-intervention.

Despite it being possible to argue for different definitions of the criterion of coercion, it is quite far from the classic perception of coercion as forcible and dictatorial to define coercion as the manipulation of the voters' opinion forming environment. Such a definition would require a development of the principle of non-intervention. The principle of non-intervention is mainly important as a part of customary international law and is as such determined by state practice and *opinio juris*. Currently, there are no indications of neither state practice nor *opinio juris* supporting this wider interpretation of coercion and non-intervention as manipulation of the opinion forming environment. Hence, advocating for coercion as opinions being formed in a manipulated environment has more of the characteristics of a *lex ferenda* discussion. Such a discussion will follow in the next section. The definition of coercion as forcible coercion threatening of consequences would therefore most likely be a more correct description of the legal position of today.

4.6 The Future of the Criterion of Coercion

4.6.1 Including Electoral Cyber Interference Aiming to Manipulate Voting Behaviour in the Definition of Coercion

Despite the slight ambiguity of the results it is unlikely that the criterion of coercion and thereby the principle of non-intervention would be applicable to electoral cyber interference aiming to manipulate voting behaviour today. However, it is possible that the principle will adapt to the current

technological possibilities and in the future include cyber voter manipulation.[212]

The principle of non-intervention is a part of customary international law and can as such evolve. The principle could therefore develop to include types of cyber operations that might not be within the scope of the principle today. This does, however, require the development of state practice and *opinio juris* that include voter manipulation in the definition of coercion. An issue is that it in general takes decades for customary international law to adapt to new phenomena which would result in a long period of legal unclarity. However, there are cases where the development of customary international law has been more rapid, but in those cases consistent state practice is essential. Small deviations are, however, not an obstacle, but more frequent deviations must be classified as violations by other states for the state practice to be considered consistent. There is no specific number of states that must engage in the practice before customary international law is developed, but it is essential that the states are diverse regarding geopolitics and legal systems. Specially affected states must also have indicated their approval of the customary international law, which in the context of cyber interference are the states with the most developed technology.[213] Additionally, there must be clear indications of *opinio juris*, which might be difficult to determine.[214]

The principle of non-intervention has already developed from only being applicable to territorial sovereignty in the nineteenth century to become applicable to other areas of state sovereignty such as political sovereignty in the twentieth century. The development was a result of the increased co-operation between states which created possibilities for subtle and effective interventions without the use of force.[215] It should therefore be possible for the principle to develop further.[216]

A challenge to the development of customary international law regarding cyber interference is the hesitance of states to reveal state practice (neither as victims nor as interveners) and the operations generally lack visibility. Furthermore, states are in general careful about articulating an opinion regarding the legality of such interference, partly due to its own activities. Hence, the ambiguity concerning the legality could be in the interest of the states and would hinder the development of customary international law.[217]

---

[212] Cf. Kilovaty (n 6) 151; Tsagourias (n 38).
[213] Schmitt and Vihul, 'The Nature of International Law Cyber Norms' (n 46) 40-41.
[214] Schmitt and Vihul, 'The Nature of International Law Cyber Norms' (n 46) 42.
[215] Philip Kunig 'Intervention, Prohibition of' (Max Planck Encyclopedias of Public International Law 2008) Para 6.
[216] Kilovaty (n 6) 170.
[217] Schmitt and Vihul, 'The Nature of International Law Cyber Norms' (n 44) 43-44.

Despite there being a possibility for customary international law to develop to include voter manipulation, such a development is not inevitable and the benefits of such a development is disputed. The possibility of regulating influence operations has been questioned by Hollis, due to the operations cognitive dimension and the difficulties regarding evidence, causation and motivation. Despite voter manipulation becoming illegal, it is not certain that the prohibition would have any real effect.[218]

4.6.2 Replacing the Criterion of Coercion

A suggestion by Kilovaty is to replace the criterion of coercion with a criterion of disruption.[219] Acts that are disruptive but not coercive can still threaten the sovereignty of a state, which the principle of non-intervention is intended to be protecting.[220] This would result in the relevant question being if the electoral interference aiming to manipulate voting behaviour disrupts the internal or external affairs of another state.[221] The replacement is combined with a requirement of only acts that succeed in disrupting the internal or external affairs of the target state should be considered illegal and that intent also is required. The assessment should be done on a case-by-case basis and include an assessment of the invasiveness.[222] Despite the addition of the criterion of disruption, the principle of non-intervention would most likely still not be applicable to some forms of voter manipulation, for example propaganda and disinformation campaigns.[223]

Replacing the criterion of coercion with a criterion of disruption is, according to me, not a certain quick fix. A criterion of disruption would clearly be more adapted and easier to apply to cyber voter manipulation despite maybe not including all such acts. To require the interference to succeed in being disruptive creates a difficult situation regarding proving the effect of the interference, a complication noticed by Hollis. In a situation where a prohibition contains criteria impossible to prove to be fulfilled, the prohibition becomes useless. However, one can also argue that just because it is hard to implement a prohibition, that is not reason enough to let wrongful acts be legal.

[218] Hollis (n 169) 44.
[219] Kilovaty (n 6) 169.
[220] Kilovaty (n 6) 172
[221] Kilovaty (n 6) 169.
[222] Kilovaty (n 6) 173.
[223] Kilovaty (n 6) 178.

Although some might want electoral cyber interference aiming to manipulate voting behaviour to constitute a violation of the principle of non-intervention, the development of international law is just not there yet. If it ever will be, is impossible to predict. The future fate of the criterion of coercion and thereby the principle of non-intervention will depend on the will of the states, and that still remains to be determined.

5 Findings and conclusions

5.1 The Exclusion of Electoral Cyber Interference Aiming to Manipulate Voting Behaviour from the Definition of the Principle of Non-intervention

Insecurity regarding the legality of cyber voter manipulation, increases the risk of conflict resulting from misunderstandings or misperceptions between states. To reduce the risk of such conflict, it is important to clarify the current legal position.

Defining coercion as forcible or dictatorial, a threat of consequences, would have to be described as the traditional interpretation of the principle of non-intervention. In the aim of adapting the principle to the technological developments of cyberspace, the suggestion of defining coercion as the lack of freedom of choice due to the voters' opinions being formed in a manipulated environment has been made. Besides the legal literature, which is only a subsidiary source of law in international law, there are no indications that coercion and consequently the principle of non-intervention should be interpreted in that modern way. There are no conventions including such a definition and no indications of state practice and *opinio juris* supporting such an interpretation. Support of the interpretation in case law does not seem to exist either. Therefore, it seems that the correct definition of the criterion of coercion would be the traditional one of forcible or dictatorial intervention with a threat of consequences to make the target state act in a certain way. In this definition, electoral cyber interference aiming to manipulate voting behaviour, is not included. Therefore, such interference does not constitute a violation of the principle of non-intervention.

5.2 Implications of the Definitions of Coercion

The objective of the principle of non-intervention is to protect the sovereignty of states from being limited by other states. It can, however, be concluded that either one of the definitions of coercion protects and limits the freedom of states. Defining coercion as forcible coercion with threat of consequences exclude voter manipulation from the scope of the principle of non-intervention and make the scope of the principle narrower. Defining coercion

as manipulating the voters' opinion forming environment includes voter manipulation in the scope of the principle of non-intervention (according to the holistic approach) and makes the scope wider. By widening the scope, independent electoral processes in potential target states are protected from electoral interference by the principle of non-intervention. This enables the voters to make a truly free choice. Such a wider scope does, however, limit the freedom of foreign affairs of potential interfering states. Acts that would be legal today, such as changing trade or development aid policies, would violate the principle of non-intervention. This would narrow the possible course of action of a state trying to strengthen its interests which are affected by the politics in other states.

With a narrower scope of the principle of non-intervention, states are freer to promote domestic interests by promoting decisions that favour the interest of the interfering state, when the decision is affected by the policies of the target state, without fear of violating the principle of non-intervention. Such a narrow scope would, however, limit the freedom of the target state. The electoral processes in the target states would not be truly free, since the opinion of the voters are misleadingly altered to benefit the interfering state, possibly at the expense of the electoral state.

A wider scope would protect the state targeted of voter manipulation while a narrower scope would protect the interfering state. The question of whether electoral cyber interference aiming to manipulate voting behaviour should be included in the scope of the principle of non-intervention therefore becomes a question of who to protect.

5.3 Potential Future and Inclusion in the Scope of the Principle of Non-intervention

Today the great powers and mainly Russia are the primary alleged perpetrators of large-scaled voter interference. To perform electoral cyber interference aiming to manipulate voting behaviour, the interfering state must be a high technological state. Cyber interference aiming to affect voter behaviour is far less costly than more physical interventions, but it still requires resources and only states able to spare bigger amounts of money can perform meaningful influence operations. While bots are becoming more sophisticated, human 'trolls' are still more convincing and human assets are also needed to hack and strategically distribute information.

The target state must also be a high technological state. For electoral cyber interference to have a real effect, the target state must be cyber dependent and the voters must mainly get their political information from the internet. To reach such level of cyber dependence the target state must be relatively well developed. Voter manipulation also requires the target state to have a well-functioning democracy. The manipulation will not have any influence on the politics in the target state if the state lack election systems or if the elections are corrupt. This is most likely an explanation to why the main targets of electoral cyber interference aiming to manipulate voting behaviour, so far, have been western democracies.

The technological development is rapid and the internet connectivity and dependence in the world is increasing. This will probably result in a shift of target and interfering states. Less developed states will become easy and rewarding targets with the increased connectivity. The lack of internet experience, maybe combined with a relatively newly developed democracy, would be an ideal target where voter manipulation might result in great effect. States previously targeted by proxy wars might find themselves targets of an influence war where the elections and consequently the governing of the state is determined by foreign cyber great powers. More states will also get the ability to perform electoral cyber interference aiming to manipulate voting behaviour themselves.

With electoral cyber interference aiming to manipulate voting behaviour becoming more sophisticated, the risk of the manipulation resulting in actual effects on the outcomes of elections is impending. Levin has shown that partisan electoral interference historically in general resulted in a three percent impact and there are indications that the belief in fake news during the 2016 United States election campaign correlated with democrats not voting for Clinton.[224]

An equally pressing issue is that the increased knowledge of the ongoing voter manipulation, besides maybe reducing the effect of the interference, might result in undermining the trust in the democratic process with declining voter turnout as a result.

Despite preventive actions being taken by promoting source criticism and revealing the sources of trolls and fake news, a criminalisation of cyber voter manipulation might give the states the tools necessary to curb the foreign influence. A criminalisation would result in the remedies available in

[224] Ch 1.2.1., 8. and ch 1.2.2., 6-7.

international law being possible to invoke, such as countermeasures and legal processes, which might have a deterrent effect.

While defining coercion as the threat of consequences would be the most appropriate definition in the current legal position, one can hope that the development of international law will result in a wider scope, including large-scaled electoral cyber interference aiming to manipulate voting behaviour. How voter manipulation is to be included is a question that would require further research. However, the probability of the development of a global or at least wide-spread multilateral treaty or of an independent norm of customary international law directed at voter manipulation does seem unlikely. A development of the scope of the principle of non-intervention, either by widening the definition of the criterion of coercion or by replacing it, could be a more practical and efficient solution.

Bibliography

Literature and Scholarly Articles

Aloupi N, 'The Right to Non-intervention and Non-interference' (2015) 4 Cambridge J Int'l & Comp L 566

Baade B, 'Fake news and international law'(2018) 29 ELIJ 1357

Bergtora Sandvik K, 'Law in the militarization of cyber space: framing a critical research agenda' in Karsten Friis and Jens Ringmose (eds), *Conflict in cyber space: theoretical, strategic and legal perspectives* (Routledge 2016)

Buchan R, 'The International Legal Regulation of State Sponsored Cyber Espionage' Anna-Maria Osula and Henry Rõigas (eds) *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016)

Corstange D and Marinov N, 'Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention' (2012) 56 AJPS 655

Damrosch L F, 'Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83 Am J Int'l L 1

Gill T D, 'Non-intervention in the Cyber Context' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publication 2013)

Gray C, *International law and the use of force* (3rd edn, Oxford University Press 2008)

Hamilton L, 'Beyond Ballot-Stuffing: Current Gaps in International Law regarding Foreign State Hacking to Influence a Foreign Election' (2017) 35 Wis Int'l LJ 179

Henriksen A, *International Law* (2nd edn Oxford University Press 2019)

Higgins R, 'Intervention and international law' in *Intervention in world politics* Hedley Bull (ed) (Clarendon Press 1986)

Hoffman S, 'The problem of intervention' in *Intervention in world politics* Hedley Bull (ed) (Clarendon Press 1986)

Hollis D, 'The Influence of War; the War for Influence' (2018) 32 Temp Int'l & Comp LJ 31

Jamnejad M and Wood M, 'The Principle of Non-intervention' (2009) 22 LJIL 345

Kilovaty I, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information' (2018) 9 Harv Nat'l Sec J 146

Kohen M, 'The principle of non-intervention 25 years after Nicaragua' (2012) 25 LJIL 157

Kunig P, 'Intervention, Prohibition of' (Max Planck Encyclopedias of Public International Law 2008)

Levin D H, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (2016) 60 ISQ 189

— 'A Vote for Freedom? The Effects of Partisan Electoral Interventions on Regime Type' (2019) 63 *JCR 839*

Lucas G, *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare* (Oxford University Press 2017)

McDougal M S and Feliciano F P, 'International Coercion and World Public Order: The General Principles of the Law of War' (1958) 67 Yale LJ 771

Moore M, *Democracy hacked: political turmoil an information warfare in the digital age* (Oneworld Publications 2018)

Nowak C, 'The changing law of non-intervention in civil wars – assessing the production of legality in state practice after 2011' (2018) 5 JUFIL 40

Ohlin J D, 'Did Russian Cyber Interference in the 2016 Election Violate International Law' (2017) 95 Tex L Rev 1579

Oppenheim L, *Oppenheim's International Law: Peace,* vol 1 (Robert Jennings and Arthur Watts eds, 9th edn, 1996)

Pawlak P, 'Confidence-Building Measures in Cyberspace: Current Debates and Trends' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016)

Sanders B, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 CJIL

Schmitt M N, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 Chi J Int'l L 30

— (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)

Schmitt M N and Vihu L, 'The Nature of International Law Cyber Norms' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016)

— (ed), *Tallinn manual 2.0 on the international law applicable to cyber operations: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence* (2nd edn, Cambridge University Press 2017)

Shaw M N, *International law* (8th edn, Cambridge University Press 2017)

Terry P C R, 'Don't Do as I Do - The US Response to Russian and Chinese Cyber Espionage and Public International Law' (2018) 19 German LJ 613

Vincent R J, *Nonintervention and International Order* (Princeton University Press,1974)

Walton D N, *Informal logic: a handbook for critical argumentation* (Cambridge University Press 1989)

— *Fundamentals of Critical argumentation* (Cambridge University Press 2006)

Watts S, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' in Jens David Ohlin, Kevin Govern and Claire

Finkelstein *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015)

Winfield P H, 'The History of Intervention in International Law' (1922-1923) 3 Brit YB of Int'l L 130

Woolley S C and Howard P N (eds), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford University Press 2018)

Yifeng C, 'The Customary Nature of the Principle of Non-Intervention: A Methodological Note' (2014) 2 Renmin Chinese L Rev 319

Ziolkowski K, 'General Principles of International Law as Applicable to Cyberspace' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publication 2013)

Other Secondary Sources

'Cambridge Analytica' (Geneva internet platform, DigitalWatch Observatory) <https://dig.watch/trends/cambridge-analytica> accessed 12 December 2019

'Methods of Foreign Electoral Interference' (*EUvsDisinfo,* 2 April 2019) <https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/> accessed 2 January 2020

Barela S J, 'Cross Boarder Cyber Ops to Erode Legitimacy: An Act of Coercion' (Just security, 12 January 2017) <https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/> accessed 27 December 2019

Gunther R, Beck P A, Nisbet E C, *Fake News May Have Contributed to Trump's 2016 Victory* (March 8 2018 Ohio State University) <https://assets.documentcloud.org/documents/4429952/Fake-News-May-Have-Contributed-to-Trump-s-2016.pdf> accessed 14 December 2019

Tenove C and others, 'Digital Threats to Democratic Elections: How

Foreign Actors Use Digital Techniques to Undermine Democracy' (Centre for the Study of Democratic Institutions, UBC January 2018) <https://democracy2017.sites.olt.ubc.ca/files/2018/01/DigitalThreats_Report-FINAL.pdf> accessed 9 December 2019

Tsagourias N, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' (EJIL: Talk!, 26 August 2019) <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/#more-17430> accessed 4 December 2019

Walker S, 'The Russian troll factory at the heart of the meddling allegations' *The Guardian* (St Petersburg 2 April 2015) <https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house> accessed 4 January 2020

Official Documents

Conference of American States

Convention on Rights and Duties of States adopted by the Seventh International Conference of American States, Montevideo 26 December 1933

Office of the Director of National Intelligence

Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Election*. (Intelligence Community Assessment 6 January 2017) <https://www.dni.gov/files/documents/ICA_2017_01.pdf> accessed 6 January 2020

Organization of African Unity

Organization of African Unity (OAU), *Charter of the Organization of African Unity*, 25 May 1963

Organization of American States

Organization of American States (OAS), *Charter of the Organisation of American States*, 30 April 1948

United Nations

UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 24 October 1970, A/RES/2625(XXV)*

UNGA, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty,* 21 December 1965, A/RES/2131(XX)

UNGA, *Draft Declaration on Rights and Duties of States*, 6 December 1949, A/RES/375

UNGA*, Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes :* resolution / adopted by the General Assembly, 15 December 1989, A/RES/44/147

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI

Table of Cases

International Court of Justice

Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America) (Merits) [1986] ICJ Rep 14

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (Merits) [2005] ICJ Rep 168

Permanent Court of International Justice

Décret de nationalité promulgués en Tunisie et au Maroc, avis consultative (advisory opinion) 1923, C.P.J.I. séries B, No. 4