Influence operations in cyberspace

On the applicability of public international law during influence operations in a situation below the threshold of the use of force

Pijpers, B.M.J.

Publication date
2022

Chapter 1

CHAPTER 1: INTRODUCTION

In the first section of this chapter the setup of the research is explained including the main research question and limitations. The second part of the chapter clarifies core themes such as cyberspace and influence operations.

Section 1.1.: Research Set Up

"Revolutions are most unsettling when least expected"[1]

1.1.1. Introduction

Ever since the presidential election of the United States of America (US) of 2016 a recurrent question dominating the news has been whether these elections had been tampered with.[2]

Questions have been raised about how these elections were manipulated, and to what end? 'What could have been done to prevent it? And against whom were these actions directed and with what instrument?' An urgent need for answers was felt, not in the least by political entities discontent with the result of the 2016 US presidential election.[3]

But more importantly, in the legal context, questions have been raised by those disconcerted with the international character of the interference in this domestic political affair undermining the legitimacy of the elections[4] and constituting a potential violation of

1 Henry Alfred Kissinger, *World Order* (New York: Penguin Press, 2014). p. 41.

2 See for example: Michael Doran, "The Real Collusion Story," *National Review*, March 13, 2018.; Nick Penzenstadler, Brad Heath, and Jessica Guynn, "We Read Every One of the 3,517 Facebook Ads Bought by Russians. Here's What We Found," *USA Today*, December 14, 2019.

3 See: Eric Chenoweth, "The Alarming Story That Won't Go Away," The American Interest, 2018, https://www.the-american-interest.com/2018/06/04/the-alarming-story-that-wont-go-away/.

4 Steven J Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion," *Just Security*, 2017.

international law.[5] According to articles in the news[6] and governmental publications,[7] the 2016 US election was influenced by a Russian cyber campaign conducted amongst others by Russian military intelligence services,[8] thereby favouring the Republican candidate Donald Trump, and undermining his Democratic opponent, former Secretary of State Hillary Clinton.[9] The media also mentioned the Trump campaign team hiring Cambridge Analytica – an outside actor - to influence US voters with a latent preference for Trump to actually go and vote,[10] making use of the activities on Facebook via the virtual identities of potential voters on the internet.[11] In this way, persons received targeted and biased news persuading or luring them to vote, and more precisely, to vote for the Republican presidential candidate Trump.

But the campaign to influence the 2016 US presidential election should not be seen in isolation as there are numerous 'cyber influence operations'[12] exacerbating the issue of intrusive cyber operations against sovereign States or the integrity and legitimacy of democratic processes of a State.[13] In 2014/5 data were stolen from the US Office of Personnel Management in which China was identified as – though not accused of being– the main suspect.[14] In 2015 the German *Bundestag* was reportedly hacked by the Russian 'Fancy Bear'-group and has remained an occasional target ever since;[15] Cambridge Analytica was not only active during the US

5 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?," Texas Law Review 95 (2017): p. 1579.

6 See for example: Michael Isikoff and David Corn, "'Stand down': How the Obama Team Blew the Response to Russian Meddling," Yahoo News, 2018, https://www.yahoo.com/news/stand-obama-team-blew-response-russian-meddling-100024634.html?guccounter=1.; Carole Cadwalladr, "I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," *The Guardian*, March 18, 2018.

7 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 2017., p. ii; Office of the Special Counsel US Department of Justice, "Indictment of the Grand Jury for the District of Columbia," 2016, https://www.justice.gov/file/1080281/download.

8 Michael N Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law*, 2018, https://ssrn.com/abstract=3180631. p. 34; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." (2017), pp. 2-3.

9 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." p. 1.

10 See Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions - The New York Times," *New York Times*, March 17, 2018.; Jane Mayer, "New Evidence Emerges of Steve Bannon and Cambridge Analytica ' s Role in Brexit," New Yorker (Newsdesk), 2018.

11 Roberto J. González, "Hacking the Citizenry?: Personality Profiling, 'Big Data' and the Election of Donald Trump," Anthropology Today 33, no. 3 (2017): p. 10.

12 Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," International Conference on Cyber Conflict, CYCON 2016–August (2016): p. 115.

13 Marie Baezner and Patrice Robin, "Cyber and Information Warfare in Elections in Europe," 2017. pp. 9-14.

14 See Dustin Volz, "Data Breaches At U.S. Office Of Personnel Management Were Preventable, Investigation Finds," The Huffington Post, 2016, https://www.huffingtonpost.com/entry/opm-data-breach-investigation_us_57cfcf69e4b06a74c9f1903b?guccounter=1. Although the FBI had accused the Chinese PLA of hacking the OPM, the Chinese government has denied any involvement. No indictment was announced against the hackers due to lack of evidence. In August 2017 a Chinese person was arrested for creating malware that is also linked to the OPM hack.

15 See: "German Parliament Cyber-Attack Still 'Live,'" BBC, 2015, https://www.bbc.com/news/technology-33093895.; Thorsten Severin and Andrea Shalal, "German Government under Cyber Attack, Shores up Defenses," 2018, https://www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8.

presidential election but previously they had allegedly supported the 'Leave-camp' during the United Kingdom (UK) 2016 referendum on European Union (EU) membership (the so-called Brexit-referendum);[16] while in May 2017 the French presidential election was affected when gigabytes of data were stolen from Macron's presidential team.[17] Foreign interference continued, albeit that the influence campaign against the US 2018 mid-term election was allegedly countered.[18] The influence operations of the Russian Federation (RF) during the 2020 US presidential election were more subtle in nature but persistent nonetheless.[19]

The actions by Russian intelligence services, China or even by Cambridge Analytica might not appear right in a political sense. The question is whether these actions are prohibited according to international law, considering that this type of action falls below the threshold of the use of force. The complexity related to the query whether it is permissible to influence the elections of another State via cyberspace and hence interfere in the political system of a sovereign State will be the main topic of this research.

1.1.2. State-level influence operations in cyberspace

Influencing as such is a common everyday activity,[20] in the commercial world but also in international relations: States with different opinions on topics such as human rights, the environment or gender will want to persuade others to modify their views and behaviour. In general terms, the verb 'to influence' means to affect or change how someone develops, behaves or thinks.[21] However, it can also be extended to reinforcing, changing or sustaining existing behaviour.[22]

For the purpose of this thesis, 'influencing' will be researched as a political act at the level of interaction between States. An influence operation in that context is an expression of a power relationship. Influencing another State actor, whether an opponent, neutral or

16 Adam Satariano and Nicholas Confessore, "Cambridge Analytica's Use of Facebook Data Broke British Law, Watchdog Finds," *New York Times*, November 6, 2018. See also: Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (Random House, 2019).; Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper, 2019).

17 Jean Baptiste Jeangene Vilmer, "Successfully Countering Russian Electoral Interference," *CSIS Briefs*, 2018, 1–6. p. 1.

18 "Cyberspace Solarium Commission," 2020. p. 29; Ellen Nakashima, "NSA and Cyber Command to Coordinate Actions to Counter Russian Election Interference in 2018 amid Absence of White House Guidance," *The Washington Post*, July 18, 2018.

19 Michael N. Schmitt, "Foreign Cyber Interference in Elections," *International Law Studies (Naval War College)* 97, no. 739 (2021). pp. 740-741; Office of the Director of National Intelligence, "Foreign Threats to the 2020 US Federal Elections," 2021. pp. 1-5; United States Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," 2021.William Marcellino et al., "Foreign Interference in the 2020 Election," 2020. p. 2; Laura Rosenberger, "The Real Threat of Foreign Interference Comes after Election Day," *Foreign Affairs*, 2020.; Elisabeth Braw, "This Time, the Meddling Is Coming From Inside the House," *Foreign Policy*, 2020.

20 Joop van der Pligt and Michael Vliek, *The Psychology of Influence : Theory, Research and Practice* (London: Routledge, 2017). p. 40.

21 Cambridge Dictionary.

22 J. David Singer, "Inter-Nation Influence : A Formal Model," *American Political Science Review* 57, no. 2 (1963): 420–30. pp. 420-422.

friendly, means to convince or impose upon another actor that one's interest prevails.[23] The 2016 US presidential election is an example of a deliberate and affirmative effort to influence an audience's choice of vote thereby attempting to change their perceptions and mind-set, but also subsequently their (voting) behaviour.

Influence operations aim to alter the cognitive processes of other actors or group, thereby changing their perception, will or attitude.[24] Though this would arguably involve non-kinetic or persuasive means, influencing activities can also be manipulative, compelling,[25] or coercive.[26] Influence operations intend to lure targeted audiences into making biased judgments instead of processing incoming data in a rational manner. Having biased judgments means that audiences were deflected in using cognitive and social heuristics due to a time restraint or due to the use of specific framed content (among others disinformation). These techniques are conducive to reflexive responses, which circumvent the deliberate understanding and autonomous decision-making altogether, thereby manipulating the target audience. The characteristics of cyberspace, especially via deliberately exploiting social media to magnify and amplify are conducive to deflecting the rational mind toward cognitive and social heuristics resulting in biased judgments.

The aim of influence operations and the characteristics of cyberspace are well suited for foreign election interferences.[27] States can be targeted by remotely executing manipulative influence operations from abroad, thereby fostering national interest and strategic goals while ensuring plausible deniability. Foreign election interference will therefore serve as the object of research. State-led influence operations have the purpose to further or protect the national interests.[28] States make use of their instruments of power – such as diplomacy, information, the military, the economy, culture and knowledge - to bolster the protection of their interests or foster them.

23 And if the other actor already has the same view or behaviour, the influencer will use capacity to reassure the existing behaviour. Singer. p. 421. See also: Joseph S. Nye Jr., "Protecting Democracy in an Era of Cyber Information War," *Belfer Center*, 2019. p. 4.

24 Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations." p. 114.

25 Thomas C Schelling, *Arms and Influence*, *Harvard University. Center for International Affairs*, Affairs., (New Haven SE - viii, 293 pages 23 cm: Yale University Press, 1966). pp. 69-78. Compellence is the ability on one State to coerce another State into action, i.e. change its position or policy, usually via a threat of engagement.

26 Eric V. Larson et al., *Foundations of Effective Influence Operations*, 2009. p. xii.

27 Duncan B Hollis and Jan Neutze, "Defending Democracies via Cybernorms," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Duncan B. Hollis and Jens D. Ohlin (Oxford University Press, 2021). pp. 315-317; Fergus Hanson et al., "Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections," 2019. p. 8.

28 Kissinger, *World Order*. pp. 9, 66 and 366/7.; Larson et al., *Foundations of Effective Influence Operations*. p. xii.; Schelling, *Arms and Influence*. p. 12.; Brandon Valeriano, Benjamin M Jensen, and Ryan C Maness, *Cyber Strategy : The Evolving Character of Power and Coercion*, *Oxford University Press* (New York, NY SE - xii, 305 pages : illustrations ; 25 cm: Oxford University Press, 2018). p. 6.

The relationship and interaction between States is regulated by public international law, during conflict as well as peacetime.[29] This thesis assesses influence operations during peacetime that are below the use of force and outside armed conflict;[30] The legal basis that regulates when and how States may resort to force - the *jus ad bellum* - as laid down in customary international law and recognised in Articles 2(4) and 51 of the UN Charter is therefore not applicable to this research.[31]

Assertive operations that do not cross the threshold of the use of force can nonetheless violate other legal obligations of international law including the sovereignty of States.[32] This research is therefore concerned with the rules and principles governing the relations between States, particularly with respect to sovereignty and the prohibition of intervention in case of foreign elections interferences. The study will not focus on individual State responsibility.[33]

It is commonly accepted that international law, governing the relations between States, also applies to cyberspace.[34] Cyberspace is a new domain which is not a threat in itself. To the contrary, cyberspace creates numerous opportunities and is therefore dominated by commercial and communicative usage,[35] ranging from emails, blogs on YouTube to targeted

29 PCIJ, The Case of the S.S. Lotus (France v. Turkey) - Judgment, Series A Collection of Judgments 1–79 (1927). no 10 at 18 "International law governs relations between independent States."

30 Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (Cambridge University Press, 2020). pp. 59-65.

31 Neither is the International Humanitarian Law (IHL) or jus in bello. IHL is applicable during an armed conflict or situation of war, regardless of its origin. Should influence operations occur in the context of an armed conflict, the legal framework IHL will additionally apply. See also: Paul A.L Ducheine et al., "Towards a Legal Framework for Military Cyber Operations," in Cyber Warfare: Critical Perspectives, 2012, 101–28. pp. 112-113. The legal doctrine related to the interpretation of laws that govern the same situation: *lex specialis derogate legi generali*. See for instance: Legality of the Threat or Use of Nuclear Weapons - Advisory Opinion of 8 July 1996, ICJ Reports (1996). Para 25, p. 18; Christopher Greenwood, "The Relationship between Jus Ad Bellum and Jus In Bello," Review of International Studies 9, no. 4 (1983): 221–34. p. 232.

32 Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice," *The American Society of International Law* 112, no. 4 (2018): 583–657. pp. 638-640; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second ed. (Cambridge, United Kingdom ; SE - xli, 598 pages ; 24 cm: Cambridge University Press, 2017). p. 17.

33 Other rules and principles include self-determination and due diligence. Both will be excluded from this research. Due diligence is excluded as the thesis relates to affirmative and offensive influence operations to which the principle of due diligence of the State is less relevant. Self-determination is excluded since the thesis relates to States and not people. From more on both see: Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 55-57; Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law," *Texas National Security Review* 3, no. 3 (2020). p. 7 (note 24); Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?" pp. 1595-1598; Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 3, 90-117.

34 See: United Nations General Assembly, "Resolution of Establishment of UN GGE - A/RES/73/226," *UN*, 2019.; United Nations GGE 2013 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/68/98," 2013. p. 8.; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. pp. 3-4; Hollis and Neutze, "Defending Democracies via Cybernorms." p. 318.

35 O'Connell and Arimatsu report that "cyberspace is conceived of first and foremost as space for communication and economic activity, international law on the use of force is seen by some as largely irrelevant for cyber security". They take the analogy of chemical weapons in this case: Mary Ellen O'Connell and Louise Arimatsu, "Cyber Security and International Law," *Chatham House: International Law: Meeting Summary*, 2012. p 6; See also Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Atomic Scientists* 75, no. 4 (2019): 187–96. p. 6.

marketing on social media platforms[36] such as Twitter and Facebook.[37] Whilst most activities in cyberspace are regular and of a legitimate private or commercial nature, some appear to be less harmless.[38] The latter may incorporate cyber-bullying, cyber-crime, cyber-espionage, the theft of intellectual property as well as an internationally wrongful act such as the use of force on or via the ICT (information and communication technology) infrastructure.[39]

Activities in cyberspace related to manipulating or undermining elections include tampering with voting machines or elections results through operations in cyberspace, but may also encompass subtler forms of exercising influence on the perception and ingrained preferences of voters.[40] All these cyber-related activities below the threshold of the use of force[41] taking place in or making use of cyberspace are only permitted in the relationship between States, if they comply with rules and principles of international law, especially the (customary international) rules of sovereignty and non-intervention. According to public international law, the sovereignty of a State including its territorial integrity and political independence must be respected.[42] Likewise, States should refrain from intervening in other States' right to exercise control of its internal affairs.

Though it is generally accepted that cyberspace is governed by existing (international) law, *how* international law applies to cyberspace has not yet fully crystallised.[43] This is partly due

36 A definition of social media would be: "Social network media refers to internet connected platforms and software used to collect, store, aggregate, share, process, discuss or deliver user- generated and general media content, that can influence knowledge and perceptions and thereby directly or indirectly prompt behaviour as a result of social interaction within networks", see: Thomas Elkjer Nissen, "#TheWeaponizationOfSocialMedia," 2015. p. 39.

37 Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," 2018. p. 21.

38 Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, 2013. p. 3; Lin, "The Existential Threat from Cyber-Enabled Information Warfare." Lin speaks about the 'dark side' of information technology, p. 6.

39 See also Netherlands National Cyber Security Centre, "Cyber Security Assessment Netherlands - CSAN 2019," 2019. pp. 15-19, the CSAN highlights that the digital threat is permanent; cybercrime continues; and alludes that the most significant threats are sabotage and disruption by nation-States.

40 Robert B Cialdini, *Influence: The Psychology of Persuasion*, Rev. ed. (New York SE - xiv, 320 pages : illustrations ; 24 cm: Harper, 2007). p. 11.

41 Operations short of war can also referred to as 'soft war'. See: Michael L Gross, Tamar Meisels, and Michael Walzer, *Soft War : The Ethics of Unarmed Conflict*, *Cambria Press*, First edit (Cambridge, United Kingdom SE - xvi, 268 pages ; 23 cm: Cambridge University Press, 2017). p. 1.

42 Paul A.L. Ducheine, "Militar Cyber Operations," in *The Handbook of the International Law of Military Operations*, ed. Terry D. Gill and Dieter Fleck, 2nd ed. (Oxford University Press, 2015). pp. 465-470.

43 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 66.; Brian Egan, "International Law and Stability in Cyberspace," *Berkeley Journal of International Law* 35, no. 1 (2016). p. 4; Zhixiong Huang and Kubo Mačák, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches," *Chinese Journal of International Law* 16, no. 2 (2017): 271–310. P. 279. Though some not only ask 'whether', 'how', but also 'why', see d'Aspremont warning not to let legal interventionalism prevail, in Jean d'Aspremont, "Cyber Operations and International Law: An Interventionist Legal Thought," *Journal of Conflict and Security Law* 21, no. 3 (2016): 575–93. pp. 592-593; Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," in *Governing Cyberspace*, ed. Dennis Broeders and Bibi van den Berg, 2020, 45–64. p. 45.

to the fluidity, anonymity, novelty and boundlessness of cyberspace.[44] These challenges, in turn, prompt legal questions including those on the conditions when assertive influence operations would arguably cross the line between legitimate interference and unlawful intervention?[45]

It can even be suggested that the development of law and cyberspace is far from being synchronic.[46] Or, as the UK Attorney General Jeremy Wright remarked during a speech on *Cyber and International Law in the 21st Century*, 'one of the biggest challenges for international law is ensuring it keeps pace as the world changes'.[47] Hence the rapidly evolving nature of cyberspace indeed raises questions about 'exactly how international law applies to this domain'.[48] Numerous issues are still unresolved:[49] discussions and negotiations in the United Nations Group of Government Experts (UN GGE) on the applicability of international law in cyberspace are often frustrated by differences in interpretation between the US, China and the RF.[50] Though there is consensus on the fact that the UN Charter as a whole applies to cyberspace, specific topics including due diligence or countermeasure remain unsettled.[51]

44 International law – including IHL - can incorporate new dimensions of warfare, such as Air warfare and the use of Nuclear weapons. See the Legality of the threat or use of nuclear weapons, Advisory Opinion of the International Criminal Court, Reports, p 266 of 8 July 1996.

45 Michael N Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," Chicago Journal of International Law, 2018, pp. 39-53.; Steven Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber," in *New Technologies: New Challenges for Democracy and International Law*, 2019, 1–27. p. 9; Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," in *Cyber War: Law and Ethics for Virtual Conflicts*, 2015. pp. 255-256.

46 Ministery of foreign affairs of the people's republic of China, "International Strategy of Cooperation on Cyberspace," 2017. The Chinese International Strategy for Cooperation on Cyberspace 2017 (p.4) States on the one hand that: "as a basic norm in contemporary international relations, the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also include cyberspace." On page 6, under the heading of "developing a system of international rules' however it states that "China supports formulating universally accepted international rules and norms of state behaviour in cyberspace within the framework of the United Nations (...)". Barnsby identifies a gap between the "accelerated pace of change in cyberspace" versus the "glacial speed at which conventional law develops". Robert E Barnsby, Shane R Reeves, and Give Them, "Give Them an Inch , They'll Take a Terabyte : Human Rights Law Chapter" 1, no. 2011 (2017). p. 1529.

47 Jeremy Wright, "Cyber and International Law in the 21st Century," 2018. Speech delivered at Chatham House on 23 May 2018. https://www.chathamhouse.org/event/cyber-and-international-law-21st-century.; see also: Roy Schondorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *EJIL*, 2020, 1–9.

48 Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *AJIL Unbound* 111 (2017): 207–12. p. 207.

49 Harold Hongju Koh, "International Law in Cyberspace," *Faculty Scholarship Series* 4854 (2012): 1–9. in Harvard International Law Journal (online), Vol 54, pp. 7-9, but see also Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly*, no. June 2010 (2011): 81–99. p. 81.

50 The fifth round of the UNGGE in 2017 even concluded without consensus and therefore without a final report with the issues of self-defence and the applicability of IHL as the most contested issues. See also: Eneken Tikk and Mika Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy," *Jyväskylä: Cyber Policy Institute*, 2017. p. 32; Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." p. 33.

51 United Nations GGE 2015 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174," vol. 12404, 2015. See also: Michael N. Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," *Texas Law Review* 95 (2017): 1639–70. pp. 1642-1643; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 40; Michael N. Schmitt, "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis," *Just Security*, 2019.; Dennis Broeders, "The (Im) Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG :

A seminal effort on how to apply existing international law to cyber operations was executed by an international group of experts facilitated by NATO.[52] The result of their work, the so-called 'Tallinn Manual', contains 154 rules in the second iteration of 2017, amplified with observations and opinions - including dissenting ones - of the experts, giving guidance to legal, civil and State actors. Many States have provided input into the manual and welcomed the result, but it is too early to conclude whether States will apply the interpretation of the manual. There is insufficient State practice and the legal opinions of States (*opinio juris*) occasionally deviated from the Tallinn Manual.[53]

The lack of clarity on how to interpret public international law in cyberspace has generated a legal hiatus but also allowed room for differences of interpretation when applying public international law to cyberspace.[54] The overarching question on how – not whether - international law applies in cyberspace is therefore a persistent, difficult and certainly complex one referred to as a 'grey area' which will require 'further investigation', and 'warrant additional research'.[55]

1.1.3. Staging the problem

Activities in cyberspace below the threshold of the use of force will not violate the jus ad bellum but this does not render them lawful. Cyber operations that do not reach the level of the use of force can nonetheless violate customary international law regarding sovereignty and non-intervention.[56] Despite their commitment to the idea that public international law applies to cyberspace,[57] actors (State and non-State) can easily make use of the virtual and boundless characteristics of cyberspace to influence the political system of another

A Mid-Process Assessment," *Journal of Cyber Policy*, 2021. pp. 1-2; Michael N. Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace," *Just Security*, 2021. Under 'UN Efforts to Address International Law and Cyberspace'.

52 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual reflects existing law (*lex lata*) and is not intended to serve as a 'best practice' guide.

53 Efrony and Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice." pp. 584-585; Though the Netherlands Supreme Court regarding State responsibility for the Dutchbat in the Srebrenica enclave made reference to Rule 17(a) of the Tallinn Manual regarding effective control in its verdict. See: Parket van de Hoge Raad, ECLI : NL : PHR : 2019 : 95 (2019). Bullet 4.16.

54 Hollis and Neutze mention four challenges in this respect: State silence; existential debates; interpretative disputes; and attribution standards, Hollis and Neutze, "Defending Democracies via Cybernorms."p. 318; Different interpretations in law can –in extremis- even be used as a weapon. According to Dunlap, cyberspace is especially prone to this: "cyber operations present a confounding lawfare issue, mainly because State practice— so important to the evolution of international law— remains underdeveloped in the area". Charles J Dunlap, "Lawfare," in *National Security Law & Policy*, ed. John Norton Moore, Guy B. Roberts, and Robert F. Turner, 3rd ed. (Carolina Academic Press, 2015), 823–38. p. 827.

55 See e.g. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 66.

56 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 68 (6), p. 330.

57 See e.g. The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 2011, p. 9.

sovereign State, which is exacerbated by conflicting interpretations on the application of international law to cyberspace.[58]

The lack of clarity in the interpretation of public international law related to activities in cyberspace can undermine and violate the sovereignty the States and can potentially even affect the international legal order which in turn is an infringement of the vital interests of many States.[59]

In summary, due to conflicting interpretations of international law when applied to cyberspace, affirmative or assertive influence operations in or via cyberspace could undermine the sovereignty of the State and subsequently, that of the entire international legal system based on States.

1.1.4. Goals of this thesis

The goal of this research is to contribute to the legal understanding, interpretation and applicability of public international law related to influence operations conducted by States in or via cyberspace.

More specific, the academic relevance is to assess how the existing principles and rules of sovereignty and non-intervention apply to the new feature of cyberspace and the influence operations executed therein.[60] In a sense, this thesis is triggered by the numerous remarks of scholars[61] that more research is required on this topic as 'the existing legal framework seems inadequate to deal effectively with cyber operations (...)'.[62]

58 Nikola Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War," Obrana a Strategie (Defence and Strategy) 14, no. 2 (2015): 73–86, p. 74; Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." p. 7 referring to a liberal or a restrictive 'strategic option'.

59 The international rule of law is one of the six national security interests of the Netherlands, see: Netherlands National Coordinator Terrorism & Security, "National Security Strategy," 2019. p. 4; See also: German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace," 2021. p. 1.

60 See, Corn and Taylor, "Sovereignty in the Age of Cyber." p. 203; Eric Jensen, "Cyber Sovereignty: The Way Ahead," *Texas International Law Journal* 50, no. 2 (2015): 275–304. p. 304; Schmitt and Vihul, "Respect for Sovereignty in Cyberspace." pp 1669-70.; Barrie Sander, "The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations," 2019, 1–21. p. 2.; Efrony and Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice." p. 584.

61 Hemen Philip Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21stCentury," *Baltic Journal of Law and Politics* 10, no. 1 (2017): 1–34. p. 1.

62 Kosmas Pipyros et al., "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare," *Information and Computer Security* 24, no. 1 (2016): 38–52. p. 38.

The lack of clarity, disputed interpretations or even gaps in legal coverage related to cyber activities can create (unwanted) leverage for States,[63] or political systems, to act against other States.[64] Societal and political relevance is to enhance transparency and predictable Stately behaviour in cyberspace by gaining knowledge of what is allowed and what is not, on the basis of the knowledge of how existing law is to be interpreted in cyberspace.

This thesis furthermore aims to contribute to the discourse within the military realm and should be seen as a vehicle to broaden the military perspective and seek opportunities away from the inherent tendency to find solace in kinetic capacities and capabilities only. Given the proper mandate, Armed Forces (including intelligence) could execute, support and enforce cyber activities below the threshold of the use of force and, conversely, should also be capable of providing some degree of protection against malicious cyber activities aimed at undermining the stability and security of the State.

1.1.5. Structure and Methodology

Given the description of the situation, the problem as presented, and the aspiration to provide more granularity on what the limits of permitted State conduct are, with respect to the rules and principles of sovereignty and non-intervention, the main research question is:

> *Which rules and principles of public international law apply to States conducting influence operations in cyberspace affecting outcomes in another political system (RQ)*

This thesis is based on desk research, and the approaches to answer this question and the ensuing follow-up questions is two-fold. On the one hand the research explores the mechanisms of influence in the relation between States. On the other hand, the thesis analyses which rules and principles of international law apply to States, executing influence operations, and when the rules of sovereignty and non-intervention are violated.

Though the research covers elements of studies on cyberspace, political science and law, the core academic research applies a legal descriptive and analytical methodology based on existing law (*lex lata*).

After describing and defining core tenets including the notions of influence and cyberspace in Chapter 1, Chapter 2 discusses the concept of influence operations in cyberspace and

63 Eneken Tikk, "International Law in Cyberspace : Mind the Gap," *Cyber Policy Institute*, no. March (2020). pp. 8-11.

64 Or as Schmitt states: "certain States are embracing legal ambiguity as a force multiplier in their cyber operations". Michael N Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," (2018), p. 66.

what techniques can be used to influence another State. This chapter answers the first sub-question:

> *What are the characteristics of influence operations, what mechanisms of influence can be applied and how does cyberspace affect influence operations? (SQ1)*

First, the concept of influence operations in cyberspace will be described in a multi-disciplinary way making use of theoretical insights from political science, social science, communication studies and cognitive psychology. Based on the dynamics of social behaviour Chapter 2 describes what techniques can be used to influence other actors.

Chapter 3 provides an insight into the theoretical legal framework. The legal framework is the core academic research, covering the rules and principles of public international law[65] applicable to States executing influence operations. The chapter focuses on the violation of sovereignty and non-interference in international conventions, customary international law, general principles and case law. The assessment will be supplemented by considerations of academic writings such as the Tallinn Manual. In this part answers the question:

> *Identify how rules and principles of international law, related to sovereignty and non-intervention apply in cyberspace to States in their conduct with other States or political systems? (SQ2)*

The chapter starts with a legal positivist identification of the principles and rules concerning sovereignty and non-intervention based on the sources of international law including treaties, customary law, principles of law and the so-called teachings of highly qualified publicists – and doctrine.[66] International law is first appreciated in a pre-cyberspace context, based on existing treaties and customary law as described, for example, in judgment of International Court of Justice. After that, the principles and rules on sovereignty and non-intervention are assessed within the context of cyberspace, relying on secondary literature – academic literature about the application of treaties and customary international law. A description of when international law - related to sovereignty and the prohibition of intervention - is violated concludes the chapter.

The legal research method follows the modern positivist approach. When referring to international law, positivism is the reflection of rules that States have agreed upon through treaties, custom or other forms of consent.[67] Positivism implies that the laws find authority

65 Ex art 38(1) Statute of the International Court of Justice.

66 International Court of Justice, "Statute of the International Court of Justice," 2014, 1–8. See article 38; Maarten Bos, *A Methodology of International Law*, ed. Elsevier (Amsterdam: North-Holland, 1984). pp. 80-82.

67 Anne-Marie Slaughter and Steven R. Ratner, "Appraising the Methods of International Law : A Prospectus for Readers," *The American Journal of International Law* 93, no. 2 (1999): 291–302. p. 293.

in the sources they stem from, what Hart calls the rule of recognition,[68] and are less inclined to take (changing) human or natural morality or ethics into account. Laws will change based on established convention and rules of a social community. Positivism is expressed in the 1927 *Lotus* Case between France and Turkey before the Permanent Court of International Justice (PCIJ), in which it was stated that 'rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims'.[69] At the same time, based on the consensual approach of the international legal order, it can be deduced that the State's freedom to exercise its sovereignty is only limited by prohibitive rules to which the State in question has consented via conventions or is subjected to when referring to customary international law.[70]

The idea of positive law is not without criticism and, arguably, it contains hidden elements of power and interest of those drafting the rules,[71] generating an incentive to modernise traditional positivism.

The modern positivist view maintains the basic principle that law is prescriptive and normative and reflects social reality rather than reality as such.[72] The 'modern' additive to positivism is that consent is not confined to the explicit will of States. *Opinio iuris* can be broadened from the application of legal document to the signing of treaties or taking positions within international fora,[73] while State practice will not only stem from external conduct but can also spring from internal decisions.

The legal research method is based on existing rules and principles of law (*lex lata*). The research is normative, [74] interpretative and qualitative in character. This research applies the doctrinal research methodology formulating a legal framework based on the analysis of legal sources of law and uses a deductive method by which these generic rules and principles are applied to specific situations.

68 Herbert L. A. Hart, *The Concept of Law*, 2nd ed., 1994. p.100.

69 PCIJ, The Case of the S.S. Lotus (France v. Turkey) - Judgment, Series A Collection of Judgments. p. 18.

70 An Hertogen, "Letting Lotus Bloom," *European Journal of International Law* 26, no. 4 (2015): 901–26. p. 902.

71 Bernard V. A. Röling, *International Law in an Expanded World*, Contributions to the Progressive Development of International Law (Amsterdam: Djambatan, 1960). p. 15.

72 Bruno Simma and Andreas L. Paulus, "The Responsibility of Individuals for Human Right Abuses in International Conflicts: A Positivist View," *American Journal of International Law* Symposium (1999). p. 307.

73 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986). Para 188, pp. 99-100.

74 Normative is the sense that legal norms are normative in character as these describe how people and States ought to behave. See: Paul Chynoweth, "Legal Research," in *Advanced Research Methods in the Built Environment*, ed. Andrew Knight and Les Ruddock, 2008, 28–38. pp. 28-30.

Chapter 4 provides an empirical description of three actual influence operations which the Russian Federation was allegedly involved in; the 2016 UK EU referendum, and the presidential elections in the US (2016) and in France (2017). The cases will be described based on the analytical framework of influence operations resulting from Chapter 2. Chapter 4 gives an outline of how the influence techniques are used and poses the following question:

How were the influence activities executed during the 2016 UK EU referendum, the 2016 US presidential election, the 2017 French presidential election? (SQ3)

The reason for choosing these three influence operations instead of others is first, that these cases are influence operations between States, contrary to operations involving non-State entities e.g. against the World Anti-Doping Agency or Sony.[75] A second argument for this choice is the availability and accessibility of data and research conducted regarding these cases. Based on the analytic framework of influence operations of Chapter 2, the fourth Chapter explains how the techniques to influence other actors are used in actual cases.

The result of the description of the three influence operations is a range of affirmative and assertive cyber-related activities, *inter alia* (i.a.) disinformation campaigns or releasing ('leaking') of sensitive data that can be assessed against the legal framework of State conduct in cyberspace. Chapter 5 provides an analysis on how the examples drawn from the cases under discussion, are conducive to influencing other State actors. The subsequent question is therefore:

How do the mechanisms of influence apply to the influence activities in the cases under discussion? (SQ4)

After a description of the theoretical legal framework about what constitutes a violation of sovereignty and the prohibition of intervention in Chapter 3, what follows in Chapter 6 is the legal analysis of the various forms of cyber-related influence activities as displayed in the cases. In this legal analysis the conduct of the cyber-related influence activities from the cases in Chapter 4 is methodically appreciated. An assessment is then made of the degree of conformity of these influence activities with existing law as described in the legal framework of Chapter 3. The assessment may result in a more normative appreciation, whether legal gaps arise when international law concerning sovereignty and non-intervention is applied to cyberspace. The sub-question discussed in Chapter 6 is therefore:

75 DFRLab, "# PutinAtWar : WADA Hack Shows Kremlin Full-Spectrum Approach," Atlantic Council, 2018, https://medium.com/dfrlab/putinatwar-wada-hack-shows-kremlin-full-spectrum-approach-21dd495f2e91.; Kim Zetter, "The Evidence That North Korea Hacked Sony Is Flimsy," Wired, 2014, http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/.

To what extent do activities of influence operations in the cases under discussion constitute a violation of sovereignty or non-intervention? (SQ5)

In sum, the analysis of this thesis first depicts what sort of cyber-related (influence) activities were executed during the cases under discussion and explores whether these specific cyber-related activities of influence operations comply with the theoretical legal framework, hence with current international law related to violations of sovereignty and non-intervention.

The research will conclude with an overview of the results and a reflection on the way-ahead, in order to provide an answer to the main research question.

1.1.6. Points of departure

Unavoidably, this research has come up against a number of limitations. It covers literature that has come available only until mid-April 2021. The research is restricted in several other ways. Cyber-related activities during armed conflict or activities amounting to armed attack, or the imminent threat thereof, are beyond the scope of this research. Nor will it focus on espionage.[76] This research solely covers cyber-related influence operations between States in a situation below the threshold of the use of force.

The referent of the research is the State and, more specific, the interaction between States. It will not refer to persons or groups that are not affiliated to a State. The research is therefore confined to public international law, governing the horizontal relationship between States, thereby focusing on the concepts of sovereignty and (non) intervention. Consequently, national legislation will not be dealt with, neither will other international legal regimes (e.g. international criminal law). Conventions on (international) human rights law or civil and political rights will also be excluded from this thesis. Though there are relevant standards including on the right to self-determination[77] or to participation in free and fair elections these standards go beyond the horizontal relation between States.

Though the research will take the perspective of the State initiating or executing influence operations (as the 'author State' of the influence operation) it will not query the accuracy or origin of assertive influence activities of the Russian Federation or any other State, or

76 Though espionage can violate the international human rights law e.g. Article 17 ICCPR, the common legal view is that espionage does not violate international law. For more see e.g. : Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?" pp. 1582-1587; or Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart, 2019). Chapter 3, pp. 48-69.

77 Article 1 ICCPR, United Nations, "International Covenant on Civil and Political Rights" (1976).

the involvement of actors such as Cambridge Analytica. These will be considered a given.[78] Consequently, attribution will be touched upon briefly, but not discussed in depth.

Section 1.2.: Fundamentals of the Research

"Hang in there, friend.
It can only get stranger"[79]

1.2.1. On cyberspace and the virtual dimension

Cyberspace is the domain in which certain operations are executed, and can be compared to the land, maritime or air domain.[80] Therefore, cyberspace is not an instrument or a weapon as such. Rather, 'cyberspace is an enabling environment that allows actors to transmit information to large audiences at low cost, near instantaneously, through multiple distribution points, across borders and with heightened opportunities for anonymity'.[81] Cyberspace[82] has been described in many different ways,[83] such as the 'juncture of digital information and human perception',[84] the 'global digital communication and information transfer infrastructure',[85] or even 'a consensual hallucination',[86] by the novelist Gibson.

78 Diego A. Martin and Jacob N. Shapiro, "Trends in Online Foreign Influence Efforts," *ESOC Publications*, 2019. p. 3. The assumption is not moot. Martin & Shapiro have analysed 54 influence effort in 24 countries between 2013 and 2018 and 72% were conducted by Russia.

79 William. Gibson, *Neuromancer* (New York - 320 p. 22cm: Penguin Press, 2018). p. xii.

80 Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *U.S. Naval War College International Law Studies* 89 (2013): 123–56. p. 123. See also: Joseph S. Nye Jr., "Cyber Power," 2010. p. 7; François Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?," *Israel Law Review* 52, no. 3 (2019): 295–326. pp. 304-305, who argues that cyber is not a new 'legal' domain and must not be compared to land, sea or air.

81 Barrie Sander, "Democray under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections," *Chinese Journal of International Law*, no. December 2018 (2019). p 3, summarizing Lin/ Kerr's description of the information environment. See also: Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity (Forthcoming)*, 2019, 1–29. pp. 11–14; Jensen, "Cyber Sovereignty: The Way Ahead." p. 279.

82 The word was allegedly coined by William Gibson in his 1982 short story "Burning Chrome".

83 Lance Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation," *Western Journal of Communication* 63, no. 3 (1999): 382–412. pp. 382-384.

84 Michael. Heim, *The metaphysics of virtual reality*, *Computer science* (New York ; SE - XXIV, 175p. ; 20cm.: Oxford University Press, 1993). p. 150.

85 Claire Cornish, Paul Livingstone, David Clemente, Dave Yorke, "On Cyber Warfare," *Prevention* 44, no. 0 (2010): 1–4. p. 1.

86 William. Gibson, *Neuromancer*, (London SE - Harper Voyager Publishers, 2013). First published in 1984. p. 51.

A review of the literature concludes that the epithet 'cyber', is not uncontested.[87] Kuehl provides a comprehensive definition of cyberspace as: "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies".[88] In a more condensed way Koh depicts cyberspace as the 'networked information infrastructure';[89] whereas others use more functional definitions, in which cyberspace 'is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructure to work';[90] or see cyberspace interchangeable with 'the internet',[91] 'virtual reality'[92] or the digital domain.[93] But also the latter definition is disputed. The digital domain is an essential component of cyberspace as it alludes to the conversion of original data (images, sounds, videos, etc.) into a digital format and manipulated inside the computer's memory.[94] While Van Keulen reverses the argument and states that 'cyberspace (...) is the part of the digital universe which is the conceptual space which is functional to Mankind for the communication of data and information'.[95]

Cyberspace can be positioned in the information environment we live in. In order to grasp the core elements and architecture of cyberspace, first the information environment will be depicted as an environment entailing three conceptual dimensions: the cognitive, virtual and physical.[96]

87 The origin of the word cyber predates the computer era and relates to the system theory. A related meaning of cyber from which our current usage stems is the coalescence of men and machine. See also Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75–78. p. 76.

88 Daniel T Kuehl, "From Cyberspace to Cyberpower:," in *Cyberpower and National Security*, ed. Franklin D Kramer, Stuart H Starr, and Larry K Wentz (University of Nebraska Press, 2009), 24–42. p. 28.

89 Harold Hongju Koh, "International Law in Cyberspace," *Faculty Scholarship Series* 4854 (2012):. p. 6.

90 Executive Office of the President of the United States, "Secure Cyberspace Secure Cyberspace," *GOV US Executive Branch*, 2003, 2–4. p. vii.

91 Kamile Nur Seviş and Ensar Seker, "Cyber Warfare: Terms, Issues, Laws and Controversies," *2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016*, 2016. p 1; Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, no. 6 (2013): 1054–74. p. 54.

92 Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation." p. 398.

93 Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 111–28. p. 1-2.

94 Digital domain. (n.d.) Computer Desktop Encyclopaedia. (1981-2015). Retrieved February 22 2019 from https://encyclopedia2.thefreedictionary.com/digital+domain.

95 Roy van Keulen, "Digital Force : Disrupting Life , Liberty and Livelihood in the Information" (2018). p. 18.

96 Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, "Manoeuvring and Generating Effects in the Information Environment," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017*, ed. Paul A.L. Ducheine and Frans P.B. Osinga, 2017. Section 9.2.2..; CJCS, "Information Operations - Joint Publication 3-13," 2014. p. I.1. Other terms for the divide are used e.g.: human or psychological instead of cognitive, or informational instead of virtual. The Joint Publication 3-13 on informational operations defines the virtual dimension as 'informational dimension' contrary to the British doctrine.

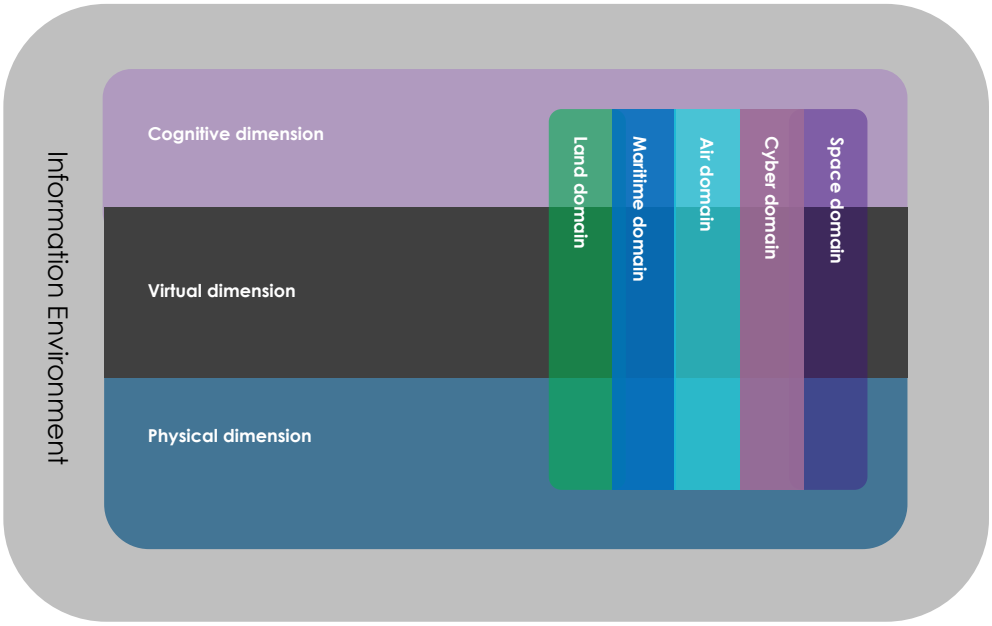

Figure 1 - 1 Information Environment

The physical dimension encompasses the globe and, furthermore, every conceivable tangible object including physical people and the 'command and control (C2) systems, and supporting infrastructure that enable individuals and organizations to create effects'.[97] The cognitive dimension is human-centric and entails our individual and collective knowledge, perception, understanding and wisdom. The virtual dimension entails where and how information is collected, processed, stored, disseminated, and protected digitally. It is the digital, imaginary reflection of the two other dimensions.[98]

The dimensions can be subdivided in layers. In the cyber-oriented model shown below,[99] the dimensions are subdivided in layers including the geographical layer (the natural earth),

97 Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." p. 5.

98 Peter B.M.J. Pijpers and Kraesten L. Arnold, "Conquering the Invisible Battleground," *Atlantisch Perspectief* 44, no. 4 (2020). pp. 10-11; Peter B.M.J. Pijpers and Paul A.L. Ducheine, "Influence Operations in Cyberspace - How They Really Work," *Amsterdam Center for International Law* 61 (2020). pp. 4-6.

99 Ducheine, Haaster, and Harskamp, "Manoeuvring and Generating Effects in the Information Environment." Section 9.2.2.; Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" (2018). See chapter 4.2.2. on Conceptualisations of cyberspace in governmental perspective for an elaborate expose on the layers of cyberspace. Other divisions use the physical, logical and social instead. See: United States Army, "Cyberspace Operations Concept Capability Plan 2016-2028," *TRADOC Pamphlet* 525-7-8, no. February 2010 (2010): 1–77. p. 8; Strate uses the distinction between the physical cyberspace containing hardware; the conceptual cyberspace entailing the logical layer or the interaction between mind and machine; and the perceptual or virtual cyberspace – the space generated by the computer-user interface though our senses. See: Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation." p. 385.

the physical layer entailing objects on earth, including buildings and persons, the physical network layer of ICT infrastructure (hardware), the logical layer of software architecture,[100] the virtual persona layer (including social media accounts), the cognitive and the social layer.

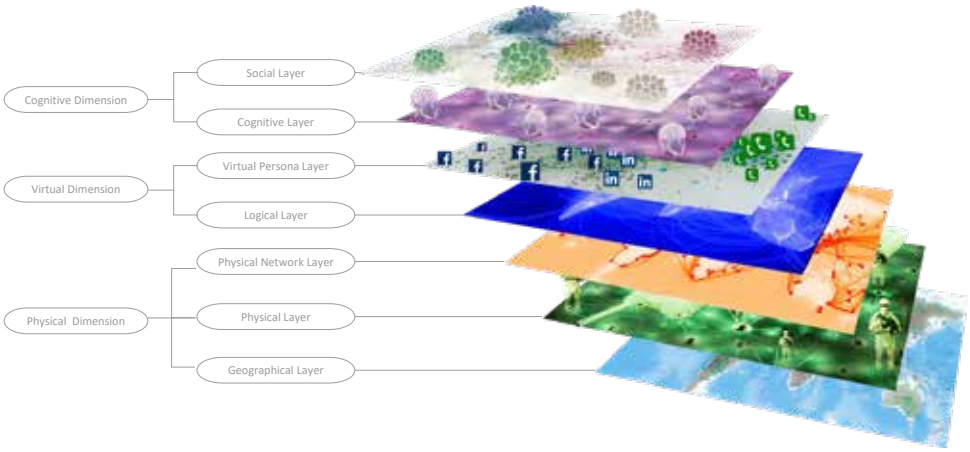

Figure 1 - 2 Information Environment - Cyber perspective[101]

The scope of cyberspace, and therefore its core elements, depends on the perspective and definition chosen. The configuration of the layers will vary, ranging from an all-inclusive approach containing all layers[102] to more restricted variations. Cyberspace can even be depicted by only singling out the virtual dimension, i.e. the layers of software and virtual persona. A distinction could be made between the technical use of cyberspace and a more political and social one – the cyber domain.[103] The latter is more comprehensive and basically entails all levels. In this research cyberspace will be used instead of cyber domain.

Ducheine et al. argue that cyberspace contains a physical as well as a non-physical or virtual element.[104] The physical side comprises the hardware (computers, servers, routers,

100 The logical layer is the software architecture comprising the of the operation (or host) system and the technical (media) system, often depicted as a model composed of several layers: application, presentation, session, transport, network, data link, physical.

101 Figure crafted by Jelle van Haaster, see: Ducheine, Haaster, and Harskamp, "Manoeuvring and Generating Effects in the Information Environment." p. 10, but based on intellectual efforts of a larger audience as alluded in note 898 of Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict." p. 173.

102 United Kingdom Ministery of Defense, "Cyber Primer (2nd Edition)," 2016. p. 5.

103 Lucas Kello, *The Virtual Weapon and International Order* (New Haven [CT] SE - xi, 319 pages ; 25 cm: Yale University Press, 2017). p. 46.

104 Paul A.L Ducheine and Jelle van Haaster, "Cyber-Operaties En Militair Vermogen," *Militaire Spectator* 182, no. 9 (2013). pp. 373-375.

and smartphones) and the physical connections between these hubs (fibre optic cables or transmission installations). Unique to cyberspace is its non-physical (or virtual) part which comprises the logical layer of software, and the virtual personas i.e. the reflections of persons and organisation in cyberspace via i.a. e-mail address or accounts on social media platforms.

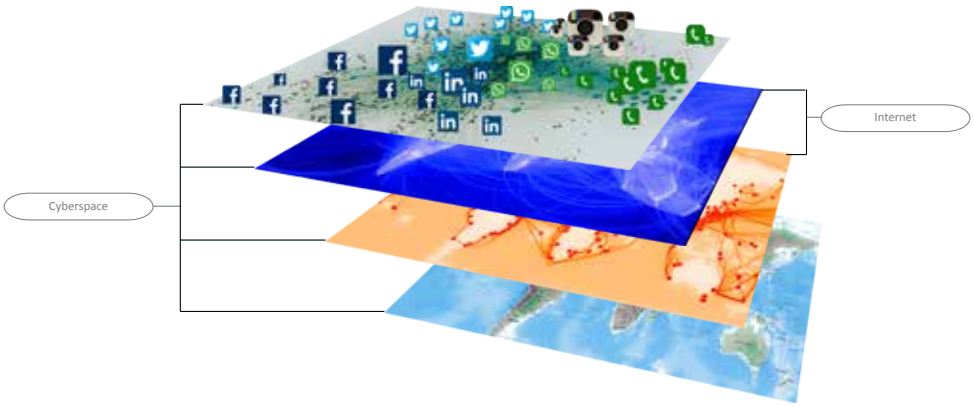

Figure 1 - 3 Cyberspace and the internet[105]

Related to the 7-layer model, cyberspace involves the virtual persona, the logical and the physical network layer. As depicted in figure 1.3., Van Haaster also takes a technical view of cyberspace, based on the internet, but argues that apart from the virtual layers and the physical network layer, the geographical layer should be included in the definition of cyberspace.[106] In both cases the cognitive dimension in not part of the technical definition of cyberspace.

An earlier description of cyberspace is given by Strate. In his view, cyberspace contains three building blocks: the physical, conceptual and perceptual. The physical part refers to "the material base of computers, monitors, disk drives, modems, wires, etc., and their users."[107] The conceptual part is the interface between the mind and the computer technology, meaning the logical layer or the man-made software but also the cyber ecology, which refers to the creation of a metaphorical 'cyberplace' including an electronic highway and virtual communities. The perceptual part refers to the impression we obtain through one

105 Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict." p. 137.

106 Haaster. p. 128.

107 Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation." pp. 384-386.

or a combination of our senses.[108] Though the labels may differ, the description of the layers does not contradict Ducheine's concept and the seven-layer model shown above.

Essential to all descriptions of cyberspace is the physical and the non-physical part. The only disputed element is whether persons or groups are part of cyberspace. The Tallinn Manual states that cyberspace consists of three layers: the physical, the logical and the social layer, and 'the social layer encompasses individuals and groups engaged in cyber activities'.[109] NATO states that "Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks".[110] Others like Tabansky, Ducheine or Van Haaster[111] include neither physical persons (human body) nor the cognitive dimension (human mind) in the description of cyberspace. According to Tabansky, cyberspace is composed of a physical, software-logic, and a data layer in which the physical layer comprises the building blocks of cyberspace such as "electrical energy, integrated circuits, processors, storage devices, communications infrastructures, copper cables, optical fibres, transmitters and receivers".[112] The question whether the cognitive and social layers or even physical persons are part of cyberspace might appear semantic. Humans, and especially their psyche, are the alpha and omega of influence operations in cyberspace, as they are for operations in the land, maritime or air domain. But when taking a technical view on cyberspace, the social and cognitive layers but also humans are not part of cyberspace not in the least because they are not the distinguishing factor of the domain.

The non-physical part can be broken up into numerous parts or segments. Strate disjoints the non-physical part, based on the mind-machine relation in a conceptual and a perceptual part. Ducheine et al. take a different stance and describes a logical layer with on top of that a layer of virtual persona.[113] All depict a similar construct but describe it differently given their individual perspectives, though only their labelling of the virtual part of cyberspace differs.

The adjective 'virtual' – and the virtual dimension as such - is not unique to cyberspace. Virtual relates to the abstraction and deconceptualisation of the physical world.[114] Virtual can be described as real but not concrete,[115] which also applies to ideologies, intellectual

108 Strate. p. 396.

109 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.Tallinn Manual 2017, p. 12.

110 Alexander Klimburg (ed), *National Cyber Security: Framework Manual*, *NATO CCD COE Publication*, vol. 6 (Tallinn: NATO CCD COE Publication, 2012). p. 8.

111 Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict." p. 127.

112 Tabansky, "Basic Concepts in Cyber Warfare." p. 77.

113 Ducheine, Haaster, and Harskamp, "Manoeuvring and Generating Effects in the Information Environment." Section 9.2.2.

114 Marilyn Strathern, "Abstraction and Decontextualization:An Anthropological Comment," in *Virtual Society? : Technology, Cyberbole, Reality*, 2002, 302–13. p. 304

115 Rob Shields, "The Return of the Virtual," in *The Virtual* (Routedge, 2002), 1–17. p 2; Kello, *The Virtual Weapon and International Order*. p. 5.

property, inventions, design, fiction and thoughts. It can even apply to a dream or a memory.[116] Virtual worlds or imagined communities[117] have been generated ever since the existence of homo sapiens.[118]

Cyberspace however, is able to create very specific virtual images (Deepfakes,[119] GANs,[120] Virtual Reality), memes,[121] persona (e.g. Facebook, Twitter or Instagram accounts) or social media communities[122] and is able to spread information in a viral and 'infectious' way[123] due to its digital, boundless character.[124] Persons can even be fully immersed in virtual environments when entering a cyber ecology or Virtual Reality created through sound, light and images by putting on goggles and a headset.[125] The logical layer of software can generate an artificial, interactive environment primarily involving vision, hearing, emotion and touch but may include all five senses.[126] The difference between the virtual world in cyberspace and the pre-digital era[127] is that in the latter case a person often realises that the virtual notion

116 Shields, "The Return of the Virtual." p. 2.

117 Benedict Anderson, *Imagined Communities : Reflections on the Origin and Spread of Nationalism*, Rev. ed. (London SE - XV, 224 p. ; 24 cm: Verso, 1991). p. 7.

118 Rosanna Guadagno et al., "Virtual Humans and Persuasion: The Effects of Agency and Behavioral Realism," *Media Psychology* 10 (2007): 1–22. p. 2.

119 Deepfakes are highly realistic digital manipulations of audio or video. Deepfakes are a result of the advances of AI whereby algorithms learn to deduce rules and replicate patterns from large data sets. See: Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War," *Foreign Affairs* Dec (2018).

120 GAN stands for "generative adversarial networks". In a GAN one algorithm (the generator) creates a model such as an image, while a second algorithm (the adversary or discriminator) sifts the artificial elements out of that image. Repeating this sequence creates a highly realistic yet fake audio or video. See also: Tero Karras et al., "Progressive Growing of GANs for Improved Quality, Stability, and Variation," *ICLR Conference Paper*, 2018, 1–26. pp. 1-2.

121 Ollivier Dyens, "The Emotion of Cyberspace: Art and Cyber-Ecology," *Leonardo* 27, no. 4 (1994): 327–33. p. 328. A meme is an independent piece of information or idea travelling in 'virtuality', and since it is contagious in nature, Richard Dawkins called it an 'idea virus'.

122 Tutku Akter and Gabriel E. Nweke, "Social Media Users and Their Social Adaptation Process in Virtual Environment: Is It Easier for Turkish Cypriots to Be Social but Virtual Beings?," *Computers in Human Behavior* 61 (2016): 472–77. pp. 472-473.

123 Including by making use of social bots. See: Emilio Ferrara et al., "The Rise of Social Bots," *Communications of the ACM* 59, no. 7 (2016): 96–104. p. 103; Kristina Lerman, "Information Is Not a Virus, and Other Consequences of Human Cognitive Limits," *Future Internet* 8, no. 2 (2016): 1–11. pp. 7-8.

124 "Although virtual worlds have existed for millennia, modern digital technology has advanced them qualitatively and quantitatively", thus Guadagno et al., "Virtual Humans and Persuasion: The Effects of Agency and Behavioral Realism.", p. 2; Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (2017): 211–36. pp. 211 & 221-223.

125 Gabriele Pizzi et al., "Virtual Reality, Real Reactions?: Comparing Consumers' Perceptions and Shopping Orientation across Physical and Virtual-Reality Retail Stores," *Computers in Human Behavior* 96, no. February (2019): 1–12., p. 1.; Jim Blascovich, "A Theoretical Model of Social Influence for Increasing the Utility of Collaborative Virtual Environments," 2004, 25–30. p. 26.

126 Fulcher, J. (2009). User interface issues in multimedia. In Margherita Pagani (ed), "Encyclopedia of Multimedia Technology and Networking (2nd Ed.)," *Hershey, PA: Idea Group Publishing 2005*, 2009.M. Ch. 201; Lin, "The Existential Threat from Cyber-Enabled Information Warfare." p. 13; Fabiana Zollo et al., "Emotional Dynamics in the Age of Misinformation," *PLoS ONE* 10, no. 9 (2015): 1–21. p. 10.

127 Or as Lin argues: "But more so today than at any earlier point in human history, human beings are vulnerable to information warfare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magnitude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia." Lin, "The Existential Threat from Cyber-Enabled Information Warfare." p. 8.

('the government' or 'a dream') is not concrete. Whilst for a cyberspace-based virtual reality, which is a 'synthetic representation of a natural or imagined environment',[128] the difference is more difficult to make.[129] In a virtual dimension the conception of what is true and what is not alters.[130] Moreover, it can even be argued that the transformative power of social media and cyberspace changes the nature and practice of human interaction including our political communication.[131]

Furthermore, social media allows sensationalist content, irrespective of source or factuality. Actors on social media can deliberately manipulate and amplify audiences by sharing misleading, deceptive or incorrect information that this audience perceives as real. Social media actors make use of algorithms to distribute fake and exaggerated news, and the sharing of the news is amplified by the use of automated bots consistently repeating news.[132] The false and sensational news websites and automated bots[133] 'are crucial tools in digital propaganda attacks—they aim to influence conversations, demobilize opposition and generate false support.'[134]

In the virtual dimension of cyberspace human senses are influenced in such a way that the difference between fiction and reality blurs.[135] The reason for this lies in the fact that the virtual concepts such as a dream is generated by the human mind while a virtual world in

128 Guadagno et al., "Virtual Humans and Persuasion: The Effects of Agency and Behavioral Realism." p. 2.

129 Modzelewski argues that, based on his research on virtual communities in cyberspace, 'there is nothing virtual about virtual reality'. In, Rafal Modzelewski, "Virtual Togetherness : Sense of Identity and Community in Cyberspace," *Crossroads: A Journal of English Studies*, no. 1 (2013): 37–53. p. 51. Dede states that 'Research suggests that the more immersive the virtual experience, as with VR, the higher the individual's belief in truly experiencing the objects and environments in the digital setting they are interacting with'. Chris Dede, "Immersive Interfaces for Engagement and Learning," *Science* 323, no. 5910 (2009): 66–69.; See also Pizzi et al., "Virtual Reality, Real Reactions?: Comparing Consumers' Perceptions and Shopping Orientation across Physical and Virtual-Reality Retail Stores." p. 2.

130 Glenn F. Cartwright, "Virtual or Real? The Mind in Cyberspace," *The Futurist*, 1994. pp. 23-25; Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election." pp. 218, 221 & 233. Allcott argues that since social media network have an element of ideological affiliation, the actors follow what they like instead of what is true. Which raises the question 'who becomes the arbiter of truth'; a striking example of the 'virtual truth' are the (Blacktivist) political rallies in the run-up to the 2016 Elections. People perceived the activities as real and interacted with 'bots' controlled by Russian agents, see: United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media," vol. 2, 2019. p. 7.

131 Johana Evelyn Montalvan Castilla and Christer Pursiainen, "Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not?," *Journal of Civil Society* 8689 (2019). p. 397; Betz and Stevens calls this 'structural cyber-power' see: David J. Betz and Tim Stevens, "Power and Cyberspace," *Adelphi Series* 51, no. 424 (2011): 35–54. pp. 48-50; Henry Farrell, "The Consequences of the Internet for Politics," *Annual Review of Political Science* 15, no. 1 (2012): 35–52. pp. 36-38.

132 Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction," *International Journal of Communication* 10 (2016). p. 1.

133 Bots is short for social robots i.e. software programs executing automated and repetitive activities in cyberspace, see: Ferrara et al., "The Rise of Social Bots." p. 96.

134 Vidya Narayanan et al., "Russian Involvement and Junk News during Brexit," *Comprop Data Memo 2017.10*, 2017. p. 2.

135 Cyber based virtual reality will be accompanied by physical changes and predicaments (see Jean Marie Normand et al., "Multisensory Stimulation Can Induce an Illusion of Larger Belly Size in Immersive Virtual Reality," *PLoS ONE* 6, no. 1 (2011). pp. 2-4.

cyberspace is a 'synthetic environment'[136] created by software.[137] Besides that, the virtual environment of social media pursues an endured engagement since its platforms are designed to be addictive.[138] A result from this is that, though the pre-internet virtual world can be used as an instrument of influence, a virtual world based on software can be manipulated in a deliberate and persistent way,[139] and targeting in a cyber ecology is more precise.[140]

The key characteristic of the virtual dimension of cyberspace is therefore the deliberate manipulation of the senses, for instance to alter the decision-making process of opponents. Following this rationale, a distinction between a conceptual (logical) and virtual persona layer of the non-physical cyberspace would be preferred, whereby the virtual layer of cyberspace is not only the reflection of the persons, groups and organisations in cyberspace but may include the virtual world – the cyber ecology[141] - that is being created: a world – in contrast to the real world – in which persons and groups interact and which consequently influences their senses via their virtual personalities.

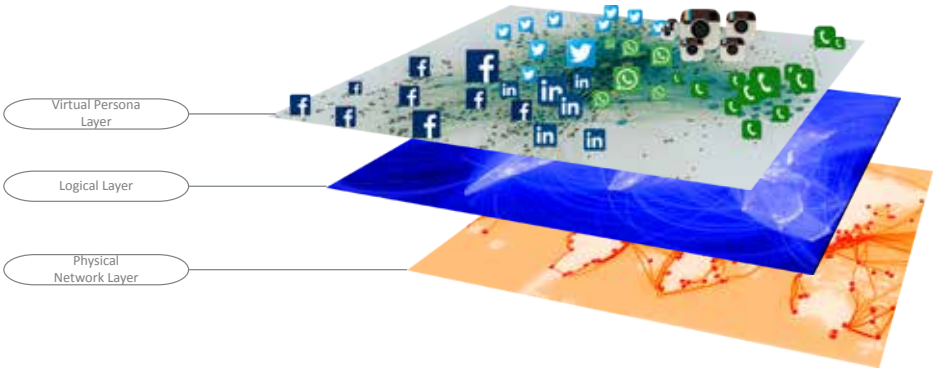

Figure 1 - 4 the minimalistic approach to Cyberspace

136 Guadagno et al., "Virtual Humans and Persuasion: The Effects of Agency and Behavioral Realism." p. 2.

137 Pizzi et al., "Virtual Reality, Real Reactions?: Comparing Consumers' Perceptions and Shopping Orientation across Physical and Virtual-Reality Retail Stores.", p. 6.

138 Hunt Allcott et al., "The Welfare Effect of Social Media," *National Bureau of Economic Research*, 2019. p. 36; P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018). p. 3. According to the author, every time a message is posted or a reaction ("like") received a burst of dopamine is released creating the need for another burst and hence another "like", or "tweet"; Peter Pomerantsev, *This Is Not Propaganda : Adventures in the War against Reality* (London: Faber & Faber, 2019). p. 161; Elaine Park, "Q&A: Anna Lembke on Smartphone Technology Addiction," The Stanford Daily, 2018, https://www.stanforddaily.com/2018/02/22/qa-anna-lembke-on-smartphone-technology-addiction/.; Vikram R. Bhargava, "Social Media: An Addictive Product Unlike Any Other," Al Jazeera, 2020, https://www.aljazeera.com/opinions/2020/10/30/social-media-an-addictive-product-unlike-any-other/.

139 This also because the virtual dimension of cyberspace does not revolve around facts but is steered by 'likes' and 'shares'. Social media is an effective platform for testing pictures, memes and stories. And the fact that smart devices are interlaced with our cognitive functioning. See: Mika Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling," 2017. p. 5.; Henry H. Wilmer, Lauren E. Sherman, and Jason M. Chein, "Smartphones and Cognition: A Review of Research Exploring the Links between Mobile Technology Habits and Cognitive Functioning," *Frontiers in Psychology* 8, no. APR (2017): 1–16. p. 13.

140 Federica; Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections," 2018. p. 2

141 Dyens, "The Emotion of Cyberspace: Art and Cyber-Ecology." p. 329.

The essence of cyberspace is the constellation of computer networks within which binary data are stored, modified and transmitted generating a virtual platform for communicative interaction. The virtual dimension represents a notional abstraction of an object, person, occurrence, system or a reality and partially overlaps but is not synonymous with cyberspace.

For the purpose of the research, the scope of cyberspace consists of three layers: (1) the physical network layer of the computers, cables and hubs – the hardware storing data and making the transfer of data possible; (2) the logical layer of software and data – the virtual logistical layer on how data are stored and what infrastructure (i.e. internet) can be created based on that; and (3) the cyber persona layer which is the virtual world created and in which the reflections of persons or groups interact. Other layers such as the cognitive or the (bulk of the) physical are also part of other domains.

1.2.2. On influence

Contrary to the generic usage, the verb 'to influence' in political science and the study of international relations signifies a power relationship between States. Influencing, in that sense, can be described as 'the ability to persuade other(s) to do what one wants, or refrain doing what one does not want'.[142] More broadly, influencing is the activity to convince, persuade or impose upon another actor that one's views or opinions prevail over those of others, but also to prevent that the view of the other actor prevails.

Influence operations can be associated with a multitude of notions,[143] including political warfare, perception management operations, soft power, or – specific to cyberspace - influence and information warfare and manipulation, soft cyber, low-intensity cyber operations or foreign influence efforts. Political warfare is 'the employment of all the means at a nation's command, short of war, to achieve its national objectives'[144], or 'the use of political means to compel an opponent to do one's will'.[145] It is mainly about the use of words, images, and it is linked to propaganda and psychological warfare. Political warfare can be combined with violence, economic pressure, subversion, and diplomacy.[146] Hollis argues that influence

142 See e.g. Simon. Reich, "The Future of International Relations : A Symbiotic Realism," in *Good-Bye Hegemony*, 2018., p. 179.

143 Jean Baptiste Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies," *CAPS of the Ministry for Europe and Foreign Affairs and IRSEM of the Ministry for the Armed Forces*, 2018., p. 18; Daniel Cohen and Ofir Bar'el, "The Use of Cyberwarfare in Influence Operations," *Blavatnik Interdisciplinary Cyber Research Center*, 2017. p. 7; Bruce Schneier, "8 Ways to Stay Ahead of Influence Operations," *Foreign Policy*, 2019, 8–13.

144 Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, 2018. Citing George Kennan, pp. 1 & 321-322. The 2018 RAND study on Modern Political Warfare and the 2009 RAND study on the Foundations of Effective Influence Operations are very similar.

145 Paul A Smith, *On PoliticalWar* (National Defense University: National Defense University, 1989). p. 3.

146 Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, D.C.: Georgetown University Press, 2020). pp. 82-85.

operations deploy resources for cognitive ends wishing the target audience to 'openly and willingly' change its behaviour,[147] thereby excluding unwilling changes and thus excluding compellence and coercion. Nye coins the term 'soft power' in contrast to hard power.[148] Soft power behaviour rests on framing agendas, attraction, co-opting or persuasion.[149] Larson states that influence operations, as a form of soft power, favour communications without resorting to use of force.[150] Soft-cyber is the use of cyber identities to influence other cyber identities over social media,[151] generating effects via, not in, cyberspace. Lin (and Kerr) argue that information warfare and influence operations 'have connotations of soft power: propaganda, persuasion, cultural and social forces, confusion and deception."[152] Moreover, they define influence operations as "the deliberate use of information by one party on the population of an opponent to confuse, mislead and ultimately influence the actions the targeted population takes. Information warfare and influence operations are hostile activities, or rather activities conducted between two parties whose interests are not well-aligned."[153] Influence operations do not constitute warfare, neither in a Clausewitzian sense nor in legal terms.[154] This is a notion similar to Wilson's definition of information operations, which argues that information operations are 'used to influence others through the dissemination of propaganda and disinformation'.[155] Watts introduces the low-intensity cyber operations which are 'actions taken short of destructive or violent attacks'.[156] Shapiro defines the foreign influence efforts as: "(i) coordinated campaigns by one state to impact one or more specific aspects of politics in another state, (ii) through media channels, including social media, by (iii) producing content designed to appear indigenous to the target state."[157]

Influence operations intend to address the attitude of a targeted audience in an attempt to change its behaviour. Though behaviour and attitude are related, there is no exclusive or causal linkage.[158] It is rather a matter of probability; a change in attitude or mindset can result

147 Duncan B. Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (2018): 31–46. pp. 35-36 & 41.

148 Joseph S. Nye Jr., "Soft Power," *Foreign Policy*, no. 80 (1990): 153–71. pp. 166-167.

149 Joseph S. Nye Jr., *Soft Power : The Means to Success in World Politics*, 1st ed (New York, N.Y: New York, N.Y. : PublicAffairs, 2004). pp. 7, 8 & 30; Nye Jr., "Protecting Democracy in an Era of Cyber Information War." p. 4.

150 Larson et al., *Foundations of Effective Influence Operations*. pp. 2-5.

151 Ducheine and van Haaster, "Cyber-Operaties En Militair Vermogen." pp. 382-383.

152 Herbert S. Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare*, 2018.

153 Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." p. 3; Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations."

154 Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." p. 4.

155 Tom Wilson, Kaitlyn Zhou, and Kate Starbird, "Assembling Strategic Narratives: Information Operations as Collaborative Work within an Online Community," *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (2018). p. 182.

156 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention.", p. 250.

157 Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 3.

158 The concept that a change in attitude results in a change in behaviour is not uncontested. Ajzen and Fishbein argue that there is a causal sequence going from belief to attitude, social norm, intention and behaviour. Icek Ajzen and Martin Fishbein, *Understanding Attitudes and Predicting Social Behavior*, ed. Martin. Fishbein (Upper Saddle River, N.J: Prentice-Hall, 1980). Icek Ajzen, "Theory of Planned Behavior," *Journal of Health Psychology* 12, no. 1 (1991): pp. 181-182. Others, like Fointaint

in certain behaviour.[159] Behaviour is the physical manifestation or activity of an actor in his environment,[160] while attitude has a psychological element related to the beliefs, emotions, knowledge and psyche of an actor, society or political system, and is passive in nature.[161]

In current literature, influencing behaviour and attitude is based on certain notions, ranging from persuasion,[162] dissuasion, credibility,[163] favouritism, nudging, deception and manipulation[164] to coercive compellence,[165] thereby making use of (the withholding of) threats and promises.[166]

In sum, there are numerous appearances of influence operations, the commonalities and hence the core tenets of influence operations are: (a) the absence of the use of force or even warfare; (b) the focus on the cognitive dimension and (c) the objective to change the behaviour of other actors directly or indirectly via a change in attitude. An influence operation can be defined as the deployment of resources for cognitive ends that foster or change a targeted audience's behaviour directly or via a change the attitude.[167] Influence operations aim to affect cognitive, psychological, and moral characteristics of a targeted audience,[168] making use of persuasion, compellence and manipulation.

---

do not believe a clear causal relation exists but urge for more research on this topics. Valérie Fointiat and Laura Barbier, "Persuasion et Influence : Changer Les Attitudes, Changer Les Comportements. Regards de La Psychologie Sociale," *Journal d'interaction Personne-Système* 4, no. 1 (2015): 1–18. p. 1 & 14. See also: Larson et al., *Foundations of Effective Influence Operations*. pp. 11-18 & 29-34.

159 Serge Moscovici, *Social Influence and Social Change*, ed. Carol Ann Sherrard and Greta. Heinz, European Monographs in Social Psychology 10 (London [etc: Academic Press [for the] European Association of Experimental Social Psychology, 1976). p. 335. The reserve can also be true since long term psychological coercion can result in undermining the moral or self-determination of a target. Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 16.

160 William Hutchinson, "Influence Operations: Action and Attitude," *Proceedings of the 11th Australian Information Warfare and Security Conference*, no. December (2010). pp. 13-14.

161 Fointiat and Barbier, "Persuasion et Influence : Changer Les Attitudes, Changer Les Comportements. Regards de La Psychologie Sociale." p. 2. «*une attitude est un état mental et neuropsychologique de préparation à l'action, organisée par l'expérience du sujet et exerçant une influence directrice ou dynamique sur sa réponse à tous les objets et à toutes les situations s'y rapportant*».

162 Persuasion can be broadly defined as any procedure with the potential to change someone's mind. See: Richard E Petty and Pablo Briñol, "Persuasion: From Single to Multiple to Metacognitive Processes," *Association for Psychological Science* 3, no. 2 (2008): 137–47. p. 137. Fointiat describes persuasion as "*revient à déplacer l'attitude initiale d'autrui vers la nôtre*" (to move the initial attitude of the others towards our). Fointiat and Barbier, "Persuasion et Influence : Changer Les Attitudes, Changer Les Comportements. Regards de La Psychologie Sociale." p. 2. In this case attitude should be recognised as a social-psychological term. Including dissuasion, see: Singer, "Inter-Nation Influence : A Formal Model." p. 424.

163 Fogg defines "persuasion as an attempt to change attitudes or behaviors or both (without using coercion or deception)" BJ Fogg, *Persuasive Technology : Using Computers to Change What We Think and Do*, The Morgan Kaufmann Series in Interactive Technologies (Amsterdam: Morgan Kaufmann, 2003). p. 8.

164 Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review* 4, no. 1 (2019): 1–52. pp. 12-28.

165 Coercion does not need to be physical in nature and is therefore not the same as 'the use of force', see infra at section 1.2.4. and: Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Bullet 20, p. 318.

166 Singer, "Inter-Nation Influence : A Formal Model." p. 426.

167 Thereby following the wording of Hollis, "The Influence of War; The War for Influence." p. 36.

168 Larson et al., *Foundations of Effective Influence Operations*. p. 3.

1.2.3. On attributes and attribution

The attributes of cyberspace as a means of communication are velocity, the lack of traditional territorial borders, its non-corporeal nature,[169] and its technological complexity.[170] Operations in cyberspace are the ultimate stealth operations.[171] Related to that, other characteristics connected with cyberspace are the paradox between, on the one hand, anonymity and, on the other, the abundance and high availability of personal data. Furthermore, the internet is conducive to swift on-line distribution of decentralised sources of information.[172] Communication via cyberspace lacks of traditional intermediates or third-party filters such as news agencies, and increasing information insecurity - what is authentic or true and what is not.[173] Many people around the world are connected to the ubiquitous internet in an interactive manner,[174] there is a low latency for news, new products but also viruses. Finally, the costs for accessing and dissemination data and information is low.[175] Cyberspace is unique in that it is manmade,[176] recent and subject to even more rapid technological changes than other domains.[177] Besides, the virtual geography of cyberspace implies 'dematerialization (everything is paperless), detemporalization (instant communication), and deterritorialization (breaking the geographical boundaries and distances)'.[178]

What is different from the other domains is that in cyberspace, and especially social media, there is no natural hierarchy between actors.[179] Everyone can communicate with everyone else, and status is less relevant.[180] The abundance and anonymity of the virtual environment

169 David J. Betz, Tim Stevens, and Bob Ferguson, "Cyberspace and Sovereignty," *Adelphi Series* 51, no. 424 (2011): p. 59.

170 Kello, *The Virtual Weapon and International Order*. pp. 2, 5-6.

171 David S Alberts and Frederick P Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd rev ed (CCRP, 1999). p. 68.

172 Cohen and Bar'el, "The Use of Cyberwarfare in Influence Operations." p. 8.

173 See also Narayanan et al., "Russian Involvement and Junk News during Brexit." p. 2., stating that 'social media favors sensationalist content, regardless of whether the content has been fact checked or is from a reliable source.'; Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election." p. 211.

174 Lin, "The Existential Threat from Cyber-Enabled Information Warfare." p. 7.; Deirdre Collings and Rafal Rohozinski, "Bullets & Blogs: New Media and the Warfighter," *Center for Strategic Leadership*, 2009, 107. pp. 9-10.

175 Lin and Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation." pp. 11-12; Ekaterina Zhuravskaya, Maria Petrova, and Ruben Enikolopov, "Political Effects of the Internet and Social Media," *SSRN Electronic Journal*, 2019, 1–32. p. 3; Henning Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law," *Israel Law Review* 53, no. May (2020): 189–224. p. 198.

176 Nye Jr., "Cyber Power." p. 1; Ebert and Maurer, "Contested Cyberspace and Rising Powers." p. 1054.

177 Nye Jr., "Cyber Power." p. 4.

178 Jackson Adams and Mohamad Albakajai, "Cyberspace: A New Threat to the Sovereignty of the State," *Management Studies* 4, no. 6 (2016): 256–65. p. 256.

179 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 198.

180 Marla B. Wadsworth and Anita L. Blanchard, "Influence Tactics in Virtual Teams," *Computers in Human Behavior* 44 (2015): 386–93. pp. 387-391.

makes it possible to ignore influence attempts which is conducive to the use of more 'aggressive influence tactics"[181].

The attributes of cyberspace make attribution challenging as it revolves around the question 'who did it'.[182] In the remit of international relations there are two sides to the coin. On the one hand, it is the intent of States that its actions or threats are attributable to them as this is the essence of exerting power, especially in the form of deterrence.[183] On the other, the actor might not want to be detected in order to cover his actions or to implement a deception operation.

Given the characteristics of cyberspace,[184] attributing a possible wrongful act to an alleged culprit may prove difficult especially in an international context. The clearest cases of attribution are overt State-led transnational cyber operations.[185] But not all cases are that easily attributable to an actor or a State, especially when there is no tangible proof of physical damage and no 'return address' for reprisals.[186]

Problems with attribution occur in different layers:[187] detection, technical authorship, legal accountability,[188] but also the political will to attribute.[189] After it has been noticed that a system is compromised, a technical and forensic investigation deals with the question which hard- and software was used and what sort of intrusion mechanism was applied. The non-linear nature of the cyberattack makes the investigation complicated but not impossible.[190]

Legal attribution is of a different nature; it involves the question whether the cyber intrusion can be linked to an actor or organisation and,[191] moreover, whether a suspected culprit (person or group) can be regarded as part of, or under control of and thus attributable to a

181 Wadsworth and Blanchard. p. 391.

182 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37. p. 4.; Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?" pp. 317-322; Florian J. Egloff and Andreas Wenger, "Public Attribution of Cyber Incidents," *CSS Analyses in Security Policy*, no. 244 (2019): 4. p. 1.

183 Rid and Buchanan, "Attributing Cyber Attacks." p. 4.

184 Yuval Shany and Michael N. Schmitt, "An International Attribution Mechanism for Hostile Cyber Operations?," *Legal Studies Research Paper Series*, no. 20 (2020): 20–36. pp. 1-2.

185 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 15 p. 87.

186 Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015): 53–67. p. 53.

187 Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges," *European Journal of International Law* 31, no. 3 (2020): 941–67. p. 2.

188 Ministerie Van Defensie, "Cyber Special," *Militair Rechtelijk Tijdschrift* 111, no. 3 (2018): 1–48. p. 45.

189 Pipyros et al., "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare." p. 49.

190 Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack." p. 56.; Harriet Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention," 2019. p. 4.

191 Pipyros et al., "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare." p. 47.

State.[192] In contrast to the technical attribution, in a legal inquiry it must be demonstrated that an object was damaged, or persons injured, that data were stolen, transformed or hijacked. In other words, what law was violated by the activity in cyberspace the perpetrator was allegedly engaged in? The legal investigation may be hampered by ambiguity whether or not public international law is fully applicable to cyber operations.[193] If in the end the violation of international law cannot be attributed to any State, an international wrongful act cannot be invoked.[194]

Ultimately, it is the political prerogative of a State to make cyber-related attack public and hold the perpetrator responsible, even without referring to the international law that applies.[195] If a damaging cyber-attack by a State is the response to a covert operation from another State, the latter might choose not to attribute the cyber-attack publicly, as it would then give away the initial covert operation. Or the culprit might turn out to be an ally, or a foe whose actions are publicly neglected, and their effects disguised in order to make the attacker think the operation failed. Political attribution can also be applied without forensic proof or legal process.[196]

1.2.4. On influence operations below the threshold of the use of force

Cyberspace benefits people, companies and States, and the metaphorical electronic highway has made the world a 'global village'.[197] The drawback of the open, boundless, transparent, and overwhelming cyberspace lies in the possible creation of just as many opportunities for actors with malicious or criminal intentions.[198] In the public media, attacks with malign intentions are often referred to as cyberattacks, though most often these 'attacks' do not

192 Schmitt, "Foreign Cyber Interference in Elections." pp. 742-744.

193 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 60.

194 United Nations, "Responsibility of States for Internationally Wrongful Acts," *Yearbook of the International Law Commission* II, no. December 2001 (2001): vol II (Part Two). Article 2 jo Articles 16, 17 & 18. Schmitt, "Foreign Cyber Interference in Elections." p. 744.

195 Sander, "The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations." p. 4.

196 Laura Galante and Ee Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *Atlantic Council* September (2018). p. 12. The 2017 French presidential hacks were attributed to Russia by the US, but France stated that no conclusive evidence could support that attribution; See also: Martha Finnemore and Duncan B. Hollis, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," *European Journal of International Law* 31, no. 3 (2020): 969–1003. p. 17; Egloff and Wenger, "Public Attribution of Cyber Incidents." p. 2.

197 In 1962, McLuhan wrote that 'the new electronic interdependence recreates the world in the image of a global village'. Marshall McLuhan, *The Gutenberg Galaxy : The Making of Typographic Man* (Toronto: Toronto : University of Toronto Press, 1962).

198 Seviş and Seker, "Cyber Warfare: Terms, Issues, Laws and Controversies." p. 1.

happen in the context of armed conflict.[199] Though cyber operations may have violent intent, most cyber activities do not reach the level of the use of force, let alone armed attack.[200]

Influence operations target the cognitive dimension aiming to alter the attitude or behaviour of a target audience. Altering or undermining the deliberate understanding and autonomous decision-making process of the targeted audience can be achieved using persuasive techniques to change the weighing (and the number) of options available, by circumventing this process in a more manipulative or compelling way, forcing a biased judgment.

Though in general influence operations apply communicative and informational means, they might include compelling means. In the notion of influence operations as dealt with in this research, the use of force is excluded.

The question is whether the *threat* of the use of force, i.e. military coercion, must either be included or excluded from this research. From an international relations perspective a division is made between 'brute' force and compellence (or coercion).[201] Coercive compellence (including via diplomatic, economic and military threats) serves a purpose as a bargaining power between two States or political systems that have a common interest.[202] Following this reasoning, the threat of the use of force as a military coercive measure is part of a generic influence operation while the use of (brute) force is not. This is so because in the latter the common interest is missing.

The legal taxonomy on the threat or use of force differs from the theory on international relations. The threat or use of force in international relations is governed by *jus ad bellum*, providing rules 'when States, as an instrument of their national policy, may resort to force'.[203]

199 One might even argue if there has even been, or will be a cyberwar. Cyberwar or cyberwarfare is much discussed in literature. The essence of the discourse revolves around the usage of 'war'. See e.g. Seviş and Seker. p. 2. Others follow a more strict and legalistic definition of war as does Thomas Rid, in "Cyberwar will not take place". His thesis is that there will be numerous hacks, cyberoperations, usage of cyber within a war, and all sorts of malicious cyberattacks, but a genuine cyberwar (i.e. an equivalent of WWII with cyber assets) will not take place; see also: Paul A.L. Ducheine and Peter B.M.J. Pijpers, "The Notion of Cyber Operations," in *Research Handbook on International Law and Cyberspace (Forthcoming)*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar, 2021). p. 6.

200 William H. Boothby et al., "When Is a Cyberattack a Use of Force or an Armed Attack?," *Computer* 45, no. 8 (2012): 82–84. p. 82, quoting: even if cyberattacks "involving military or intelligence operations could violate domestic or international law, they don't always rise to the level of a use of force or armed attack under the international law that governs the legality of the use of force, also known as jus ad bellum."; And for influence operations this would also be 'extremely unlikely', see: Dale Stephens, "Influence Operations & International Law," *Journal of Information Warfare* 19, no. 4 (2020): 1–16. p. 5.

201 Schelling, *Arms and Influence*. pp. 2-5.

202 This does not imply that the employment of coercion will generate a win-win situation. The coercer will impose its will upon another actor which will comply in order to protect a higher cause i.e. peace, economic gain or international stability. See e.g. the "Peace for our time" declaration of UK prime minister Chamberlain after the Anglo-German agreement of September 1938. The 'peace' came at a cost i.e. the 'settlement of the Czechoslovakian problem' and was not long-lasting.

203 Michael N. Schmitt, "'Attack' as a Term of Art in International Law : The Cyber Operations Context," *4th International Conference on Cyber Conflict* n/a, no. 2010 (2012): 283–93. p. 284.

Article 2(4) and Chapter VII – especially Article 51 - of the UN Charter[204] epitomise and codify this body of law,[205] intended to discourage States from the threat or use of force and instead seek peaceful ways for settling disputes.

The width of the standard regarding the threat or use of force has frequently been subject to discussion.[206] Already during the 1945 'conference on international organization' the Brazilian delegation submitted an amendment to the so-called Dumbarton Oaks proposal: "...from the threat or use of force and from the threat or use of economic measures in any manner inconsistent...etc",[207] to what later would be Article 2(4) of the UN Charter. The proposal to add economic coercion to the use of force standard was rejected. During the drafting of the 1970 Friendly Relations Declaration, the 1966 Czechoslovakian proposal, stating that every State 'has the duty to refrain from economic political or any other form of pressure aimed against the political independence or territorial integrity of any State, and from undertaking acts of reprisal'[208] was rejected as well.

The threat or use of force therefore refers to military use of force and to military coercion,[209] i.e. the threat of force. The ICJ in the 1996 *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion argues that 'the notions of "threat" and "use" of force under Article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal (..) the threat to use such force will likewise be illegal'.[210] The kind of weapon used is irrelevant in this case. The 1996 ICJ *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion further argues that the provisions of Article 2(4) do not refer to specific weapons but apply to any use of force. The ICJ is ambiguous about the legality of nuclear weapons as such,

204 Article 2(4) UN Charter: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."

205 There is some legal discourse whether there is a difference between the standard of the use of force and of an armed attack, or whether these standards overlap. The common opinion in international law is that these standards differ, see also: Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 201, p 106; United Nations General Assembly, "Definition of Aggression - Resolution 3314 (XXIX)," 1974.; Tom Ruys, "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum : Are 'Minimal' Uses of Force Excluded From Un Charter Article 2(4)?," *The American Journal of International Law* 108, no. 2 (2014): 159–210., pp. 162-163. The alternative view states that there is no difference between the use of force and an armed attack is being made, see: US position after the Nicaragua case: see Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. p. 332- 333, and Abraham D. Sofaer, "International Law and the Use of Force," in *Proceedings of the Annual Meeting (American Society of International Law)*, vol. 82, 1988, 420–29. p. 422; see also: Michael N. Schmitt and Durward Johnson, "Iranian Gunboat Harassment and the Rules of Engagement," *Just Security*, 2020.

206 Quincy Wright, "Subversive Intervention," *The American Journal of International Law* 54, no. 3 (1960): 521–35. pp. 529-530.

207 United Nations Information Organization (UNIO), "United Nations Conference on International Organization (UNCIO) - Volume III," vol. III, 1945. pp. 253-254.

208 United Nations, "Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation among States" 19, no. 19 (1969): 126. p. 17.

209 James R Crawford, *Brownlie's Principles of Public International Law*, 9th ed. (Oxford, United Kingdom: Oxford University Press, 2019). p. 720.

210 Legality of the Threat or Use of Nuclear Weapons - Advisory Opinion of 8 July 1996, ICJ Reports. Para 47, p. 246.

but unanimous on the fact that using nuclear weapons contrary to Article 2(4) is unlawful.[211] The essence is that the prohibition is related to the use of force or the threat thereof.[212] Other forms of compelling threats, such as political, economic, diplomatic but also cyber-related threats which are not executed by means of force, are (hence) not subject to the prohibition of the threat or use of force.[213]

The legal interpretation of the prohibition of the use of force which is a peremptory rule of customary international law, recognised in Article 2(4) of the UN Charters, incorporates the military threat of force.[214] Economic or political threats are not prohibited under the use of force standard,[215] which is the line of argumentation that will be followed in this research.

Influence operations in cyberspace below the threshold of the use of force can make use of activities including persuasion, manipulation and compellence, the latter of which includes economic or political threats but excludes (military) threat of force. For the purpose of this research influence operations are therefore inherently below the threshold of the threat or use of force.

211 Legality of the Threat or Use of Nuclear Weapons - Advisory Opinion of 8 July 1996, ICJ Reports. para 37-39 and 105 under A), B) and C). The ICJ is of the opinion that neither customary nor conventional international law gives any specific authorisation for the threat or use of nuclear weapons, nor is there a prohibition of it.

212 Legality of the Threat or Use of Nuclear Weapons - Advisory Opinion of 8 July 1996, ICJ Reports. Para 52, p. 247 stating: "State practice shows that the illegality of the use of certain weapons as such does not result from an absence of authorization but, on the contrary, is formulated in terms of prohibition".

213 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *Cambridge University Press*, 2013. p. 47.

214 Wright, "Subversive Intervention." pp. 528-529.

215 Or as Damrosch points out: forcible activities must be judged against article 2(4), nonforcible actions are not. Lori F. Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs," *The American Journal of International Law* 83, no. 1 (1989): 1–50. p. 5.