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 7

CHAPTER 7: CONCLUSIONS AND REFLECTIONS

In this final chapter the conclusions of the research are presented based on the key findings of all chapters in order to provide an answer to the main question of this research: *"Which rules and principles of public international law apply to States conducting influence operations in cyberspace affecting outcomes in another political system?"*

This chapter provides the key tenets that need to be taken into account when executing affirmative influence operations in cyberspace, and how international law, more specifically the rules of sovereignty and non-intervention guides these activities. After providing the key tenets related to influence operations in cyberspace, the conclusions related to sovereignty and non-intervention will be presented.

Lastly, a reflection is presented on the future of State conduct in cyberspace, in the light of the conclusions provided. The reflection will also offer options to reduce the grey zone with reference to the objective of this thesis.

Section 7.1.: On Influence Operations in Cyberspace

"Social media and its widespread adoption have changed the nature and practice of human interaction for much of the world."[1]

7.1.1. On Cyberspace

Cyberspace is part of the information environment, which contains three dimensions: the physical, the virtual and the cognitive dimension.[2] The virtual dimension is part of cyberspace. Cyberspace, as defined in this thesis, consists of three layers in total; the physical network of hardware, the logical of software and data, and the virtual persona layer.[3] Other physical appearances, territory, buildings, the human physique, but also the cognitive dimension (the mind of humans or groups) are not part of cyberspace under this definition.

1 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. 8.

2 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. pp. 5-7.

3 See § 1.2.1.

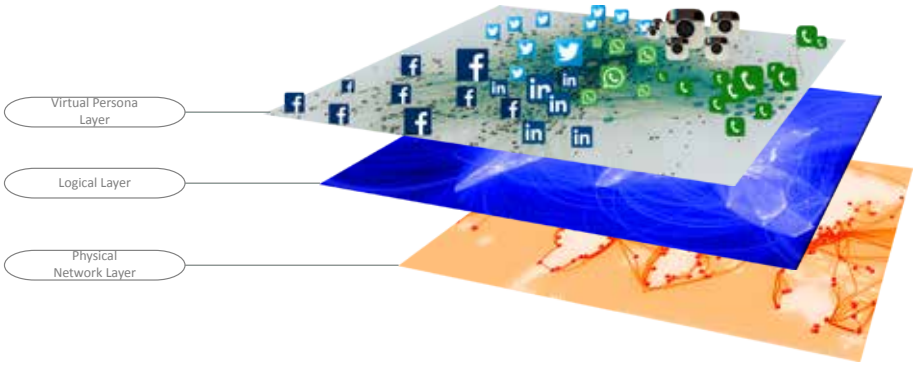

Figure 7 - 1 Cyberspace[4]

Cyber operations can target the layers in cyberspace but can also use cyberspace as a vector to affect the cognitive dimension. Activities, making use of cyberspace, can be divided into hard- and soft-cyber operations.[5] Targeting the layers in cyberspace, in order to extract or modify data, causes the denial of service or even destruction of ICT infrastructure, results in effects *in* cyberspace which are defined as hard-cyber activities. Soft-cyber operations use cyberspace as a vector or means of communication to target the cognitive dimension, hence have an effect outside -cyberspace. Soft-cyber operations use content, words, memes and footage as 'weapons', contrary to hard-cyber operations, which make use of computer codes (0/1) and data to alter cyberspace. Influence operations are inherently soft-cyber operations that can be supported by hard-cyber operations.

Based on the cases under discussion it can be concluded that:

> *Influence operations can be supported by hard-cyber operations (intrusions in the ICT infrastructure). During the cases under discussion hard-cyber operations were witnessed during the preparatory phase of an influence operation.*

4 Based on Ducheine, Haaster, and Harskamp, "Manoeuvring and Generating Effects in the Information Environment." pp. 155-179; Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" (2018). p. 137.

5 Peter B.M.J. Pijpers and Kraesten L. Arnold, "Conquering the Invisible Battleground," *Atlantisch Perspectief* 44, no. 4 (2020). pp. 12-14.

7.1.2. On Mechanisms of Influence

Depending on its intent, influence operations use persuasive, compelling or manipulative mechanisms of influence, whereas persuasive and compelling influence activities use more rational, overt and conscious techniques. However, the more the frame (framed narrative) of an influence operation relies on covert and subconscious techniques (heuristics), the more manipulative the frame will be. The conscious elements, including socially divisive topics (police violence, race, gender), are required to generate an air of realism to the influence activities, whereas subconscious heuristics and biases (stereotyping, familiarity, conformity) are needed to create reflexive responses.[6]

Persuasive influence operations are overt and conscious whereby State A (the author State) aims to change the weighing and number of options available to the targeted audience, in order for State B (the target) to make a voluntary ('willing') choice that will be beneficial to State A. Compelling influence operations cut short or circumvent the deliberate understanding and autonomous decision-making process of the targeted audiences of State B, forcing them to consciously make an 'unwilling' choice.[7] Manipulative influence operations use subconscious techniques that subvert or usurp the autonomous decision-making process. The targeted audience, often unaware of being influenced, are duped into making reflexive biased judgments based on cognitive and social heuristics.

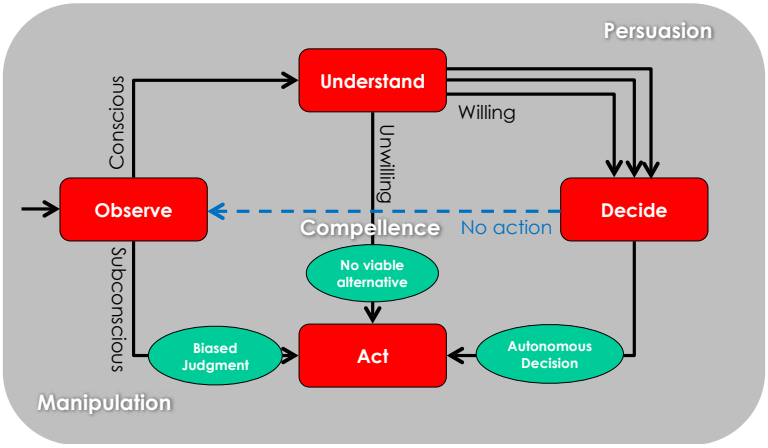

Figure 7- 2 Forms of Influence Operations

6 See also: Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56. pp. 238-243; Media Ajir and Bethany Vailliant, "Russian Information Warfare : Implications for Deterrence Theory," *Strategic Studies Quarterly*, 2018, 70–89. pp. 72-73; Keir Giles, "Handbook of Russian Information Warfare," *NATO Defence College* 9, no. November (2016): 1–90. p. 19.

7 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. 4.

The influence operations in the cases were predominantly manipulative and deceitful since (a) the content was fabricated or doctored to sow discord or worsen the socio-political divisions and polarisation of societies. By using bots and mimicking nationals (e.g. citizens of the United States (US)) or news agencies, the agents of the Russian Federation (RF) were deceitful in (b) the source of the content. Moreover, the velocity and (c) overload of information, combined with the covert nature of the influence activities and hence the inability of the targeted audience to validate the content, force them to deflect towards reflexive responses and biased judgments based on ingrained preferences and heuristics rather than rely on conscious and rational appreciations, thereby circumventing their ability to make a deliberate understanding of the information.

Influence operations are not new. The Cold War-period was infamous for extensive influence operations by the Soviet-Union and the US and their respective allies.[8] What is new is the context of cyberspace. Apart from the low costs of entry, cyberspace makes communication faster and more diffuse. Furthermore, it enables actors (State and non-State) to surgically target specific audiences with bespoke messages based on algorithms. The characteristics of cyberspace, and especially of social media, exacerbate the possibility to create an overload of information and generate a sense of urgency. Moreover, if the information is one-sided due to the use of algorithms, the targeted audience will not be able to (objectively) attach meaning to the data provided.

Based on the cases under discussion it can be concluded that:

Though persuasive activities could be detected (including foreign political propaganda), the (soft-cyber) influence operations in the casus under discussion were predominantly manipulative influence operations.

The attributes of cyberspace facilitate deflecting the rational mind toward cognitive and social heuristics, resulting in biased judgments. Actors (States) executing influence campaigns can deliberately exploit social media to magnify and repeat specific messages to which the audience is receptive.

7.1.3. On Influence Operations

In this thesis, the main characteristics of influence operations are the absence of the threat or use of force,[9] the focus on the (collective and individual layers of the) cognitive dimension,

8 For an overview see: Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020).; Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, 2018.

9 See § 1.2.2. On Influence Operations: persuasion, manipulation, coercion & Chapter 2, key findings.

with the objective to change the behaviour of other actors, directly or indirectly, via a change in attitude.[10]

While implementing the strategy of a State, influence operations conceptually follow the three-phased scheme of preparing the influence operation, executing it, and finally exploiting the cyber-related activities that have gained some success or momentum.[11] During the 2016 US presidential election RF performed all three phases of the influence operation, but an influence operation as such is not always a fully-fledged State-led operation. A State can also choose to perform solely a specific phase, or temporarily support an ongoing influence operation, if this coincides with its strategic interests. In the case of the referendum on the future of UK membership of the EU, RF influence activities focussed on exploiting social media, while in the 2017 French presidential election RF interests appeared to have waned after the limited spoils from the Macron hack. The RF was not always the initiator of the influence operations. In the 2016 UK EU referendum, they supported and enhanced existing domestic influence operations.

To exert influence State A will require a well-prepared and methodologically- executed and exploited influence operation as a strategic instrument of statecraft. Preparing an influence operation commences with the formulation of an intent based on the vital interests of the State. Its intent will reflect the attitude of State A. If State A wishes to pursue the intent, it will select instruments of power (such as diplomacy or economy). For an influence operation the informational instrument of power will be best suited, because it applies strategic narratives to undermine the deliberate understanding and autonomous decision-making capacity of (the targeted audiences of) State B.

10 Eric V. Larson et al., *Foundations of Effective Influence Operations*, 2009. p. 3; Duncan B. Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (2018): 31–46. p. 36.

11 See Section 4.1 of Chapter 4.

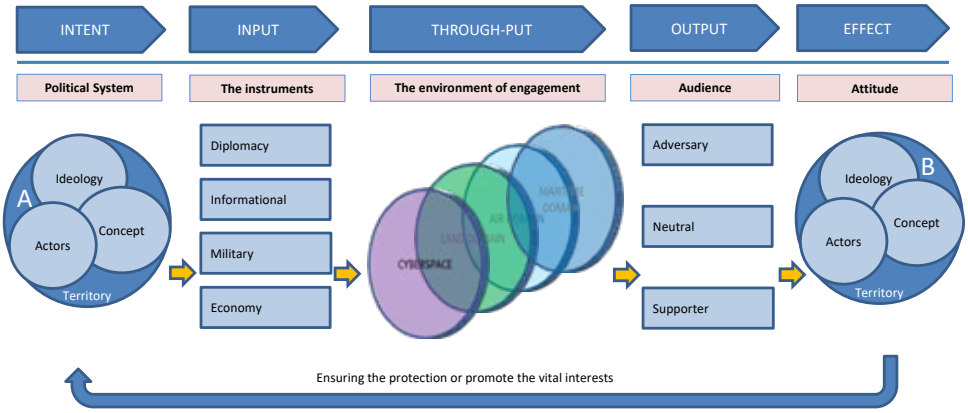

Figure 7 - 3 The framework of Influence Operations

Strategic narratives do not automatically influence the targeted audiences of State B, the content or form of strategic messaging needs to be shaped – or framed - in such a way that it fits the cognitive dimension (preference and heuristics) of that audience in order to make them receptive to the narrative. The mechanisms of influence – persuasion, compellence and manipulation – will shape the frame.[12] Forging the frames requires in-depth knowledge of the targeted audiences and society. The frames that are designed (e.g. the frame of presidential candidate Clinton being part of the American political elite and thus lacking integrity) do not need to be true but need to be framed as genuine or realistic.[13]

For this reason, hard-cyber hack operation can be used to retrieve (sensitive) data to forge the frames or the subsequent cyber-related activities (disinformation and leaking campaigns), which will be employed during the execution of the influence operation. In the run-up to the 2016 US presidential election the Clinton campaign team, the Democratic party entities DNC and the DCCC but also the election infrastructure of several American States (including Illinois), were hacked.[14] In the 2017 French presidential election the Macron campaign team was also hacked to extract sensitive data.

After preparation the influence operation is executed via cyber-related activities in which (the author) State A engages with (the target) State B. The cyber-related activities range from

12 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. 13-18.

13 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). Chapter 1 &2 on Sovereignty and Due Diligence; Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018).

14 United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 1: Russian Efforts Against Election Infrastructure," vol. 1, 2019. pp. 10-21.

the leaking of non-public information, to disinformation, trolling (defamation) or political grooming (including advertisements) campaigns, utilising cyberspace as a vector for relaying content. The content can be manipulated by what or how and in what volume it is presented. The final phase is to exploit the specific attributes of cyberspace to increase the reach and repetitive effect of those cyber-related activities to which the targeted audiences are subjected. The susceptibility can be amplified by increasing the number of social media platforms and magnified by repeatedly feeding the (fabricated) messages back into the information environment. Due to the velocity and reach of Internet the exploitation of successful cyber-related activities practically runs parallel with the cyber-related activities themselves, reinforcing the effect and exacerbating the information overload and inability to make sense of the proffered data. This will deflect the target audiences towards biased judgments based on heuristics.

Based on the cases under discussion it can be concluded that:

An influence operation is not always a fully-fledged State-led operation in which the author State performs all three phases (preparation, execution and exploitation of social media) of the influence operation. A State can also support ongoing influence operations, domestic or initiated by another foreign State. A foreign State can choose to execute a specific phase if this coalesces with its strategic interests.

Section 7.2.: On Sovereignty and Non-Intervention

"Some jurists have proposed to abolish the notion of the sovereignty of States, considering it obsolete. That is an error."[15]

After providing the key tenets related to cyberspace and influence operations, which form the context of this thesis, the following section presents the conclusion regarding sovereignty and non-intervention.

7.2.1. Sovereignty

The concept of sovereignty is 'linked to the authority of the state to control its territory and exclusively perform certain functions therein."[16] Territorial integrity and political

15 Corfu Channel (U.K v. Alb.), 1949 I.C.J. (Opinion of Judge Alvarez), ICJ Reports 43 (1949). p. 43.

16 Marko Milanovic and Michael N. Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic," *Journal of National Security Law & Policy* 11 (2020): 247–84. p. 255.

independence of a State are inextricability connected. However, for academic purposes the elements of sovereignty will be described separately.

Sovereignty can be breached if either one of the core elements of sovereignty - territorial integrity and political independence - is violated. After analysing the legal consequences of the cases under discussion in Chapter 6, this chapter addresses the implications of cyber-related influence operations for the notion of sovereignty in general.

7.2.1.1. Territorial Integrity

The assessment resulting from the legal analysis of the cases under discussion in Chapter 6 is that cyber-related foreign election infringements may violate territorial integrity. Territorial integrity was violated during the 2016 US and the 2017 French presidential election. However, this violation was not due to soft-cyber influence operations. It was breached because agents of the RF were on US territory without the latter's consent- and because hard-cyber hacks installed malware and backdoors on ICT infrastructure of several Democratic entities in the run-up to the 2016 US presidential election. Likewise, in the French case, a cloud-based device was emplaced on French ICT infrastructure to retrieve data.

Based on the cases under discussion it can be concluded that:

> *Influence operations can violate territorial integrity if foreign agents, without explicit consent of the injured State, execute influence operations from within the injured State.*

However, most influence operations are executed remotely, i.e. from outside the target State. In these operations, as also witnessed in the cases under discussion, cyberspace is used as a vector to influence the cognitive dimension of the (audiences of the) target State. Remote influence operations, as can be deduced from the cases, do not have a manifest impact on the targeted State since no harm is inflicted on the territory of the target State. These influence operations fall below the *Tallinn Manual 2.0* qualified thresholds of physical or functional damage,[17] and even below the intrusion-based threshold since no data were deleted or altered.[18]

This prompts the question of how to apply the notion of territorial integrity to remotely executed foreign influence operations that affect the targeted State via cyberspace.

17 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. pp. 20-21, rule 4 (11-14).

18 Przemysław Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach," in *Governing Cyberspace*, ed. Dennis Broeders and Bibi van den Berg, 2020, 65–84. p. 79.

Apart from unauthorised access to the territory,[19] territorial integrity is breached when State A infringes on the territory of State B without the latter's consent resulting in manifest physical or functional damage. Sovereignty, and thereby territorial integrity, in essence has a strong territorial dimension.[20]

Cyberspace, on the other hand, is only partially territorial. The physical network layer – the computers and routers – of cyberspace has a clear connection with the territory of a State.[21] While the physical network layer (ICT infrastructure) is part of the territory of the State, the virtual dimension of cyberspace is not always easy to align with the notion of territoriality[22] due to the attributes of this domain.[23] The virtual dimension of cyberspace is inherently 'a-territorial'.[24] However, based on the thresholds of the *Tallinn Manual 2.0* and resulting from the cases under discussion, hard-cyber activities targeting the virtual dimension of cyberspace can violate territorial integrity of the targeted State, especially if the software layer is directly connected to the physical network layer in a State.[25] The emplacement of malware and installation of backdoors during the hack into the Clinton campaign team, the DNC and the DCCC in the US and the installation of a virtual backup drive on the Macron campaign team's ICT infrastructure during the French election could amount to a violation of territorial integrity, based on the thresholds of both the *Tallinn Manual 2.0*.[26] and the intrusion-based approach.[27] The latter does not assess the effect of cyber-related intrusion,

19 Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *U.S. Naval War College International Law Studies* 89 (2013): 123–56. p. 124.

20 Nicholas Tsagourias, "The Legal Status of Cyberspace," in *Research Handbook on International Law and Cyberspace*, 2015, 13–29. p. 17.

21 Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace." pp. 126-127.

22 Dan Jerker B. Svantesson, "International Law and Order in Cyberspace—Cloud Computing and the Need to Revisit the Foundations of 'Jurisdiction,'" *Aspen Institute Central Europe*, no. 01 (2016).; see also the discussion on data and the virtual dimension in other legal regimes including IHL, Heather A. Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives," *Israel Law Review* 48, no. 1 (2015): 39–54.; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 92, pp. 415-420; Ido Kilovaty, "The Elephant in the Room: Coercion," *AJIL Unbound* 113, no. June 27 (2019): 87–91. p. 87.

23 As illustrated by the ongoing discourse on whether (virtual) data is an object or not. See e.g. the discourse in the context of IHL, Michael N. Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations," *International Review of the Red Cross*, 2019, 1–23. pp 8-11; Bart G.L.C van den Bosch, "Oorlog Voeren Zonder Geweld" (University of Amsterdam, 2019). Para 4.5 pp. 121 ff; Robin Geiß and Henning Lahmann, "Protection of Data in Armed Conflict," *International Law Studies (Naval War College)* 97 (2021). pp. 569-572.

24 Svantesson, "International Law and Order in Cyberspace—Cloud Computing and the Need to Revisit the Foundations of 'Jurisdiction.'" Under 'could computing and international law'. The software or data attached to a specific Internet address of a physical device (computer or smart phone), does not have to be in the same State as the physical component of cyberspace, nor does the data need to be in one place. E.g. Blockchain and TOR-networks techniques are based on a worldwide network of several thousand relays.

25 This is not always the case. Big technological companies (Google, Facebook or Twitter) are registered in State X (e.g. Alphabet in the US), while they will have large data centres in numerous places in the world (e.g. the Netherlands), see: "Google to Spend $1.1 Billion on New Data Centers in Netherlands," Data Center Knowledge, 2019, https://www.datacenterknowledge.com/google-alphabet/google-spend-11-billion-new-data-centers-netherlands.; see also the SWIFT example in Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (26)., pp. 24-25.

26 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (14), p. 21.

27 Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." p. 79.

but argues that if, due to the deletion of data or the emplacement of malware the integrity of an ICT system is breached sovereignty is violated.

Based on the cases under discussion it can be concluded that:

> *Cyberspace can be partially connected to the territory of a State based on the physical network layer. Activities that harm or damage the physical network layer will breach territorial integrity and thus the sovereignty of the injured State.*
>
> *Territorial integrity is more difficult to align with the virtual dimension of cyberspace. But, a malign remote computer intrusion (hard-cyber activity) could still breach territorial integrity if data are deleted or altered, denting the integrity of the virtual dimension.*

Hard-cyber operations target the layers of cyberspace i.e. the physical network, the logical and the virtual persona layer, which occurred during the 2016 US and the 2017 French presidential elections.

Soft-cyber influence operations use cyberspace as a vector and do not impact cyberspace. They aim to affect the cognitive dimension of the people and groups using cyberspace.[28] During the cases under discussion, these remotely executed influence operations did not cause harm or damage in a direct manner, which would suggest that they did not breach territorial integrity.

However, cyber-related activities - including remotely executed influence operations -could also affect the territory of an injured State in an indirect manner.[29] If influence operations make use of inciting content[30] and provoke demonstrations or riots, then conveying a message via cyberspace may not cause harm as such,[31] but the operation could result in civil strife or subversive behaviour which may, in an indirect manner, lead to harm or injury and thus to the loss of State's control over its territory.[32]

28 Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, 2013. pp. 193-194.

29 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 254.

30 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." p. 3.

31 United States Senate Committee on Intelligence. pp. 40-41.

32 The Capitol Hill-riots on 6 January 2021 were probably not instigated by a foreign actor but are nonetheless an example of how inciteful messages can cause physical harm. See e.g. Al Jazeera, "After Capitol Riots , Russia Slams US's 'archaic ' Electoral System," Al Jazeera, 2021.

Based on the cases under discussion it can be concluded that:

> *Remotely executed influence operations, using cyberspace as a vector, are not likely to violate the territorial integrity of another State in a direct way. But they could affect territoriality in an indirect way.*

This might be an inconvenient conclusion. However, the conclusion is specific to remotely executed operations that solely use cyberspace as a means of communication. In practice, as witnessed in the cases under discussion, influence operations are not executed in isolation but are accompanied by other activities which are not remote but take place within the injured State with hard-cyber operations or with influence operations outside cyberspace. Moreover, the conclusion above only applies to the territoriality of a State and not to sovereignty as a whole. Remotely executed influence operations via cyberspace are not directly connected to the territory of a State, but activities in or via the virtual dimension can have indirect legal ramifications if physical persons or groups are affected by the cyber operation that possibly breaches territorial integrity.[33] Legal implications can also affect the legal order and the jurisdiction of the State, which will be dealt with in the next sections.

7.2.1.2. *Political Independence*

Political independence is breached when the inherently governmental functions are violated by means of usurpation or interference.[34] The main results from Chapter 6 are that no usurpation of inherently governmental functions occurred in the cases under discussion. Nonetheless, apart from taking over State functions, there were unlawful interferences in the political independence as a result of both hard- and soft cyber operations. The (soft-cyber) influence operations in the UK and US cases interfered with the State's task to conduct elections or hold a referendum. In the French case the interference was not unlawful since the influence operation was flawed.[35]

This means that while remotely executed influence operations using cyberspace as a vector are unlikely to violate territorial integrity, they may violate the political independence of the target State. This deduction underlines Denton's remark that '(a)n interference theory is most plausible here'.[36] Denton was referring to the potential breaches of international law during the RF election infringements in the 2016 US presidential election, away from a violation of

33 Regarding the link between territory and jurisdiction see also: Tsagourias, "The Legal Status of Cyberspace." pp. 19-20.

34 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (15) p. 21.

35 Schmitt. Rule 4 (24) p. 24.

36 Allison Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign," *Boston University International Law Journal* 37, no. 171 (2019): 183–210. p. 201.

territorial integrity. Schmitt echoes this by stating that '(a) more fertile ground for finding a violation of sovereignty vis-à-vis remote cyber operations affecting another State's elections is interference with, or usurpation of, inherently governmental functions.'[37]

The basis for political independence is well-defined in the *Island of Palmas* Case, where Arbitrator Huber remarked that, '(i)ndependence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[38] This means that, as an element of sovereignty, the State has the right to exercise the State functions without outside interference.

Regarding violations of political independence in cyberspace, damage is not the overarching criterion. What is of relevance is that the breach relates to an inherently governmental function – either via usurpation or interference.

Usurpation of inherently governmental functions involves unilaterally taking over the State tasks of another State and conducting them instead of the injured State without the latter's consent. Though in the cases under discussion no usurpation was documented, this does not imply that cyber operations, especially hard-operations, are incompatible with the notion of usurpation.[39] Examples of hard-cyber operations that would amount to a violation of sovereignty due to the usurpation of inherently governmental functions are;[40] the covert search for incriminating evidence in foreign government databases, taking over the registration and selection of the candidates for public offices,[41] or taking over the electronic counting of votes after an election.[42]

The influence operations in the cases under discussion did not usurp inherently governmental functions,[43] which is in line with Schmitt arguing that 'the issue in the election context is interference',[44] not usurpation.[45]

37 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 45.

38 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards 829–71 (1928). p. 828.

39 Jens David Ohlin, "Election Interference: The Real Harm and The Only Solution," *Cornell Law School Research Paper No 18-50*, no. 50 (2018). pp. 6-8.

40 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?," *Texas Law Review* 95 (2017): 1579–98. p. 1594; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. p. 24. Brian Egan, "International Law and Stability in Cyberspace," *Berkeley Journal of International Law* 35, no. 1 (2016). pp. 13-14.

41 Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law," *Texas National Security Review* 3, no. 3 (2020). p. 38.

42 Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?" p. 1594.

43 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 201.

44 Michael N. Schmitt, "Foreign Cyber Interference in Elections," *International Law Studies (Naval War College)* 97, no. 739 (2021). p. 753.

45 See also: 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). p. 322.

Based on the cases under discussion it can be concluded that:

> *Influence operations remotely executed via cyberspace are not likely to usurp inherently governmental functions.*

Interference of political independence takes place by way of actions 'that disturb the territorial State's ability to perform the functions as it wishes.'[46] Defining interference of inherently governmental functions is challenging since these notions, both interference and State functions, 'lack granularity'.[47] There is a fine line between what is unwelcome and unlawful. Foreign election propaganda, diplomatic protest, or purchasing political advertisements, and similarly, using social media platforms to disseminate foreign election propaganda does not per se amount to unlawful interference with the political independence of another State. An overt manner of influencing could also be classed as persuasion.

The 'inherently governmental functions' are not tasks that should be protected by the State, but rather those that are not to be privatised since they are intimately related to the public interest.[48] State functions, therefore, do not cover purely commercial activities but include national defence,[49] tax collection, law enforcement[50] and conducting elections.

In the cases under discussion a plethora of cyber-related activities was executed to directly disturb the State's ability to conduct elections. These activities included deceptive disinformation and trolling campaigns, but also political advertising and leaking of sensitive data overwhelming the public sphere with one-sided information, thereby undermining the public trust in the electoral system, sowing discord and aggravating the socio-political divisions in a foreign State.

Carrying out these State functions outside one's own territory or interfere with the State tasks of another State must be presumed unlawful, and a violation of political independence, irrespective of whether these are executed in cyberspace or any other domain.

46 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 45-46.

47 Schmitt. p. 45.

48 Simon Chesterman, "'We Can't Spy... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions,'" *European Journal of International Law* 19, no. 5 (2008): 1055–74. p. 1070.

49 Schmitt argues that "law enforcement and defense of the State from external attack are inherently governmental in character." Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 45.

50 Other judicial functions such as criminal investigation and prosecution could also fall within the discretionary exercise of governmental authority, see: Chesterman, "'We Can't Spy... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions.'" p. 1071. Some argue that extraterritorial law enforcement is a violation of the prohibition of intervention, see: Maziar Jamnejad and Michael Wood, "The Principle of Non-Intervention," *Leiden Journal of International Law* 22, no. 2 (2009): 345–81. p. 372.

Based on the cases under discussion it can be concluded that:

While the context of cyberspace affects the applicability of territorial integrity, the notion of political independence remains intact and can be applied in cyberspace as well as in any other domain.

Though political independence has a territorial dimension, a breach of political independence is not dependent on territory but on the infringement of inherently governmental functions. And since remotely executed influence operations, via cyberspace, do not have a direct territorial dimension, the notion of political independence is the best option to guide State behaviour related to influence operations in cyberspace.

7.2.2. Non-Intervention

The prohibition of intervention can be violated by influence operations if these are invasive in the *domaine réservé* in a coercive manner. The *domaine réservé* relates to the internal or external affairs of a State, which includes jurisdiction over semi-public or private sectors. Coercion is the essential element of an intervention and refers to an affirmative act with the intent to deny another State its freedom of choice, and force that State to act in an involuntary manner.[51]

Persuasive influence operations, including propaganda and political advertisements will most likely not reach the threshold of coercion, while compelling influence operations are inherently coercive.[52] Most influence operations in the cases under discussion were neither persuasive nor compelling but manipulative influence operations, relying on covert and subconscious techniques. Manipulative influence operations, including foreign election infringements, could still amount to an intervention if the invasive infringement in the reserved domain is coercive by nature. In the cases under discussion an analytic tool was used to assess the coerciveness of the invasive cyber-related action, based on three elements. The coercive State aspires to a) undermine the control and autonomous decision-making process of the target State,[53] b) in an intentional and deliberate way,[54] c) with the aim to change the policies of that State. A coercive intervention does not need to succeed as a failed attempt is still coercive.

51 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (18) p. 317.

52 Though compellence (as a term of international relations) is coercive, compellence does not equal coercion as an term in the context to international law, see: 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. 56.

53 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; Jamnejad and Wood, "The Principle of Non-Intervention." p. 381; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (11) pp. 315-316.

54 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (27) pp. 321-322.

The main results from Chapter 6 are that all three cases were invasive in the reserved domain of the State, but not all infringements (both hard-cyber and manipulative influence operations) were coercive. In the French case neither the hard-cyber intrusion into the ICT infrastructure of the Macron campaign team nor the soft-cyber influence operation would amount to a coercive intervention. The legal analysis of the hacks into the Clinton campaign team, the DNC and DCC remained inconclusive, whereas the soft-cyber influence operations in the 2016 UK EU referendum and the 2016 US presidential election case did violate the prohibition of intervention.

The reserved domain is not the point of contention when assessing the application of the rule of non-intervention to cyberspace. Similar to the inherently governmental functions, the jurisdiction of the State (based on its sovereignty) applies to cyberspace as to any other domain.[55] It could even be argued that coercion as a notion with legal consequences applies to cyberspace as it does to other domains. The issue at hand is rather that the potentials to employ methods with a coercive nature or intent have increased due to cyberspace. The possibilities cyberspace offers - facilitating enhanced reach and speed at low cost - go far beyond the traditional tools,[56] such as influence operations based on (US) political warfare or (Soviet) Active Measures in the past.[57] The manipulative and deceitful techniques used during the cases under discussion were fabricated content, deceptive media outlets, impersonating domestic agents via (fake) media accounts. Moreover, leaking of sensitive data and amplifying and repeating messages on a multitude of social media platforms generates a rapid overload of one-sided information. The use of these techniques invokes a subconscious way of processing incoming data resulting in biased judgment, which in turn deprives the targeted audience (the electorate) of its freedom of a rational and deliberate choice.

Based on the cases under discussion it can be concluded that:

> *Both elements of intervention, the reserved domain and coercion, apply to cyberspace in the same way as they do to other (physical) domains.*

55 It is not said that the reserved domain of a State, based on jurisdiction, is the same as the inherently governmental function. Though they overlap, they stem from different conceptual notions. Schmitt. Rule 4 (22) p. 24; Marcelo Kohen, "The Principle of Non-Intervention 25 Years after the Nicaragua Judgment," *Leiden Journal of International Law* 25, no. 1 (2012): 157–64.p. 159.

56 Uta Kohl, "Jurisdiction in Cyberspace," in *Research Handbook on International Law and Cyberspace*, 2015, 30–54. p. 31. Kohl gives the example that in medieval Europe the Church controlled mass communication, after which the national political leaders shared the control on communication, while nowadays 'on-line actors, large and small, are contesting the control over information and ideological production' on the Internet.

57 Henning Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law," *Israel Law Review* 53, no. May (2020): 189–224. pp. 193-195.

Influence operations, including manipulative ones, can violate the prohibition of intervention as they can unlawfully interfere with the inherently governmental functions. While the threshold for an interference - 'to disturb' a State function – might be easily reached, the threshold for an intervention – coercion – is a qualified one, which is apparent from the fact that a flawed interference does not violate sovereignty, while an unsuccessful intervention can still be coercive.

Applying the notion of coercion to cyberspace does not change the nature of coercion, but cyberspace opens a plethora of activities which could be coercive, including manipulative influence operations. This in turn raises the threshold for coercion because it is traditionally based on an unambiguous act of a State, in general supported by the treat or use of force. In cyberspace these explicit attributes are lacking and therefore additional or more refined criteria could be called for. To be more precise: first, as mentioned in the *Nicaragua* Case, the 'element of coercion, which defines and indeed forms the very essence of prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action or in the indirect form of support for subversive or terrorist armed activities within another State',[58] while cyber-related influence operations are *de facto* below the level of threat (or use) of force. Second, cyberspace has significantly increased the coercive potential due to the increasing number of actors, but also because cyberspace facilitates the use of covert and subconscious activities. Third, manipulative influence operations in cyberspace are not always linear operations executed by a single State or by actors that have aligned interests.[59] Finally, due to the highly elusive methods of operating of State agents (or actors under State control) but also of loosely aligned actors, it is difficult obtain the true purpose and intent of an alleged intervention.

An unwanted development is that the complexity of cyberspace and the increased possibilities to employ manipulative techniques via cyberspace increases the complexity of, and the requirements needed to establish, coercion in cyberspace.[60] A strict application of coercion to cyber-related (influence) operations will result in the fact that coercion will only be granted when activities exerting extreme forms of coercion resemble the use of force.

58 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986). Para 205, p. 108.

59 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 241, p. 124.

60 See deliberations on this topic by Alex Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election," *Duke Journal of Comparative & International Law* 30, no. 2 (2020). pp. 373-379; Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 202; Kilovaty, "The Elephant in the Room: Coercion." pp. 89-91; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 48-53.

Based on the cases under discussion it can be concluded that:

> *The attributes of cyberspace have a weathering effect on the notion of coercion, affecting it in a negative manner and making the requirements more diverse and less tangible. The result could be that only the most severe forms of influence operations will be assessed as coercive.*

Section 7.3.: Reflections

> *Any nation's right to a form of government and an economic system of its own choosing is inalienable. Any nation's attempt to dictate the other nation their form of government is indefensible.*[61]

The goal of the thesis was to make a contribution to the reduction of the normative uncertainty which has resulted from the variance in interpretations on *how* international law should be applied to cyberspace. In this reflection an outlook will be given on the development of influence operations, on the dangers of the normative-and, finally, on the need to reduce this uncertainty including some suggestions that might facilitate the reduction.

The future of influence operations

Though the RF was exposed after the 2016 US presidential elections,[62] the number of cyber-related operations or, more specifically, the foreign election infringements have not withered.[63] In fact, after the 2016 UK EU referendum the 2016 US and the 2017 French presidential elections the number of cyber-related influence operations have increased exponentially and will be increasing,[64] both with hard- and soft-cyber operations. Moreover, having learnt from previous experiences, the techniques that are being used are getting more sophisticated and better adjusted to the context of the targeted State.[65] For example, in the 2020 US presidential election the RF shifted their cyber-related operation primarily to influence operation, while no cumbersome hard-cyber hacks were witnessed. Apart from adjusting the techniques used to target another State, foreign infringements will also be

61 Dwight D. Eisenhower, "The Change for Peace," April 16, 1953. Third and fourth bullet of his address.

62 Not least by the Mueller report and the subsequent indictments. See e.g. Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," vol. I and II, 2019. and United States District Court, Indictment (United States v Internet Research Agency LLC) (2018).

63 Schmitt, "Foreign Cyber Interference in Elections." pp. 740-741.

64 Fergus Hanson et al., "Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections," 2019. p. 5

65 The 2020 US presidential election saw a shift from hard- and soft-cyber activities to solely soft-cyber influence operations, which could indicate that RF assessed that influence operations would yield a better crop. Office of the Director of National Intelligence, "Foreign Threats to the 2020 US Federal Elections," 2021. pp. 1-2.

more successful due to the improved linguistic proficiency and cultural knowledge of the actors involved: outlets such as RT and Sputnik are able to broadcast in local languages.[66] Finally, the foreign infringements will become savvier in the legal remit. The activities deployed will deliberately stay below the threshold of the use of force and most likely also below the level of coercion.[67]

The increase in influence operations is unwanted due to effect they resort. In numerous States there is a growing distrust of traditional media, governmental institutions and, on average, cynicism has increased, which also takes shape in the unwillingness to accept election results and the scepticism toward public announcements.[68]

The danger of normative uncertainty in cyberspace

Regarding the application of international law to cyberspace, many States remain sitting on the fence.[69] Even those that have published an official legal opinion on the application of international law to cyberspace, within the context of the UN GGE or separately, often use generic terms reiterating existing law without expediting on *how* international law applies to cyberspace. It has frequently been mentioned that increased State practice will increase clarity on how international law applies. However, based on the cases under discussion and the analysis made in this thesis, the opposite might turn out to be true. The more States act in cyberspace, without a common understanding of notions related to sovereignty and non-intervention, the greater the normative uncertainty appears to be.

Over the years- the grey area of international law has not diminished. In fact, the possibilities cyberspace provides to create competition below the use of force have only increased. Compared to the traditional, physical realm, more actors are active in cyberspace-that can reach the entire globe within seconds and can penetrate the individual minds of social media users with bespoke messages. The increased uncertainty also affects the possibility to attribute malign acts to a State, and the interconnected characteristics of cyberspace generate numerous possibilities for multiple actors to converge or diverge their efforts based on randomly aligning interests, rather than on time-consuming treaty-based coalitions.

66 "Countering Kremlin's Media Influence in Europe," 2021. p. 39.

67 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 62-63.

68 For example regarding COVID-19, enhanced by foreign actors or not, see: Nina Jankowicz and Henry Collis, "Enduring Information Vigilance: Government after COVID-19," *Parameters* 50, no. 3 (2020). p. 22.

69 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." pp. 209-216.

A contribution to closing the gap

Cyberspace and the State's behaviour in cyberspace generate uncertainty. States are sceptical towards the information environment and technological and socio-political development – including the erosion of a shared public arena or even the liberal-democracy as a whole - they encompass.[70] The information environment reinforces the anarchic nature of the international system of States.[71] The legal system could give, and has given, some structure to the behaviour of States.

A grey area in the legal remit related to sovereignty and non-intervention (the two core legal notions that provide guidance to the relation between States in a peacetime situation) is therefore highly unwelcome.[72] This 'uncertainty' not only exists regarding sovereignty; some States still argue that sovereignty is not a rule but a principle in cyberspace. There is also uncertainty about non-intervention. The essential element for an intervention, i.e. coercion, is ill-defined[73] and even more elusive when applied to cyberspace.[74] Questions related to whether an intervention is sufficiently coercive,[75] or whether coercion comes in degrees of intensity or intrusiveness, are illustrative of this discourse.[76]

The grey area might be unwanted from a legal point of view, but it could be beneficial from a political point of view. As mentioned before, it is generally accepted that international law applies to cyberspace;[77] 'how' it applies is still subject to interpretation.[78] The normative uncertainty means that numerous interpretations of a rule exist. This fragmentation in the legal system can be exploited and the different interpretations of international law concerning

70 "Countering Kremlin's Media Influence in Europe." pp. 23-25; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 199.

71 Alexander Lanoszka, "Disinformation in International Politics," *European Journal of International Security*, no. 4 (2019): 227–48. pp. 233-234.

72 Nicholas Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace," *European Society of International Law Reflections Series* 9, no. 4 (2020). p. 7.

73 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 197.

74 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 196; Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law* 12, no. 5 (2001). p. 849; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." pp. 200-202.

75 Joyner and Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework." p. 849.

76 Ido Kilovaty, "The Democratic National Committee Hack: Information as Interference," *Just Security*, 2016. Under Intervention 2.0.

77 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.; 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.

78 Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." p. 34; Dennis Broeders, "The (Im) Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG : A Mid-Process Assessment," *Journal of Cyber Policy*, 2021. p. 1

cyberspace are conducive to 'cherry-picking'.[79] States can apply and interpret international law in a manner that is beneficial to their conduct in cyberspace, which could include sustainment of the current status-quo and subsequent fragmentation. The 'uneasy fit'[80] between traditional State-based international law and the a-territorial cyberspace creates tension between States regarding the desires to preserve freedom of action for oneself while developing rules to restrict the others?[81]

More granularity in the application of international law is therefore needed to decrease the variance in interpretations, and hence to align the opposing views of States. Below three suggestions are made about how some legal uncertainty can be lifted.[82] The suggestions relate to (1) territorial integrity in cyberspace, (2) the question whether sovereignty is a rule and a principle that applies to cyberspace or merely a principle, and finally (3) to the suggestion not to apply coercion too strictly.[83]

Territorial integrity and cyberspace.

The *Tallinn Manual 2.0* has provided several thresholds for assessing whether a remote cyber-related activity violates territorial integrity and causes physical damage, functional damage and infringements below functional impairment. These criteria are based on the effect the intrusion will have.

While the category of physical damage is generally accepted, also the functional impairment is well-defined and is the logical continuation of the category of physical damage in the *Tallinn Manual 2.0*.[84] The third criterion for infringements below functional damage is rather difficult to solidify; even the Tallinn Manual-experts could not reach agreement on it. There are, however, other schemes for assessing the cyber-related intrusion, such as the French position that any penetration into (French) ICT infrastructure is a violation of territory.[85] Unfortunately, this approach is as difficult to operationalise as the current third criterion of the *Tallinn Manual 2.0*.

79 Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." p. 33.

80 Kilovaty, "The Elephant in the Room: Coercion." p. 89.

81 Chimene Keitner, "Foreign Election Interference and International Law," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Duncan B. Hollis and Jens David Ohlin (Oxford University Press, 2021), 179–95. pp. 180-181.

82 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 45.

83 Without suggesting that coercion is not required in an intervention as some do, see: 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. p. 642.

84 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (13) pp. 20-21.

85 Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace," 2019. p. 8; Harriet Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention," 2019.

Roguski offers an alternative to the effect-based approach, which is more concrete than the French approach.[86] This intrusion-based approach of Roguski combines a conceptual notion with tangible implications. The concept is based on the CIA-triad, relating to confidentiality, integrity and availability of data. An intrusion that breaches the integrity of the ICT infrastructure may violate territorial integrity. Integrity of an ICT system is corrupted once data are deleted, malware is emplaced, or remote access tools are installed. In effect the intruder has violated the control the State has over objects within its territory.
The suggestion is that the intrusion-based approach can give substance to the third *Tallinn Manual 2.0* threshold related to infringements below functional impairment. The intrusion-based approach is more tangible and concrete and amalgamates the intrusion-based approach with the third Tallinn Manual threshold,[87] thus being conductive to reducing the normative uncertainty.

Sovereignty as a rule

Remotely executed influence operations that use cyberspace as a vector are not likely to violate territorial integrity. This should, however, not be seen as a confirmation that sovereignty is a mere principle of international law. Without diving too deeply into the discourse whether a principle of international law can have binding legal consequences,[88] remotely executed influence operations may violate political independence. Contrary to the notion of territorial integrity, the attributes of cyberspace have no substantial effect on political independence.

The fact that political independence may be violated via an interference on the inherently governmental functions means that influence operations, hence soft-cyber operations that use cyberspace as a vector, may violate sovereignty.

Acknowledging that sovereignty is a binding rule of international law also means that violating sovereignty may invoke an internationally wrongful act if the violation can be attributed to a State. If so, redress for the injured State is possible. These recognitions reduce the normative uncertainty and generate a more scheme how to apply international law to cyberspace.

86 Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." pp. 77-80.

87 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Rule 4 (14), p. 21.

88 See e.g. Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace." pp. 4-5 or Jeroen C. van den Boogaard, "Proportionality in International Humanitarian Law - Principle, Rule and Practice" (University of Amsterdam, 2019). p. 384.

Coercion in cyberspace

While the nature of the constituting elements of non-intervention (the reserved domain and coercion) does not change when applied to cyberspace, the possibilities cyberspace offers increases the nuances and shades of potentially coercive activities. This is a result of, among others, the multitude of actors involved in cyberspace and the possibilities of covert and subconscious activities. Many new activities have recently been witnessed in cyberspace, for example the DDoS attack on a hospital, foreign infringements of an Internet Access Point, or the attempt to gain social control via computational data and propaganda.[89] The question is whether these activities can be classed as coercive since they 'subordinate the sovereign will' of the targeted State?[90]

To circumvent the complexity of this conundrum a more normative approach[91] which favours a less strict application to coercion might be appropriate,[92] not least since manipulative influence operations are not 'particularly obvious' cases of coercion.[93] To reduce normative uncertainty the criteria for coercion need to be revisited, as is described below.

In the 2005 *Armed Activities* Case (Democratic Republic of the Congo v. Uganda), the territorial integrity, intervention and prohibition of the use of force were violated.[94] Regarding the intervention, the ICJ argued that the coercive actions of Uganda were sufficient to violate the prohibition of intervention and use of force, 'even if the objectives of Uganda were not to overthrow President Kabila'. From this it can be deduced that the overall aim of the author State does not have to be specifically defined, which is a reiteration of a rationale also used earlier in the 1986 *Nicaragua* Case.[95] Furthermore, this is underpinned by Schmitt's argument about the indirect causation of coercive effects; in other words, there does not have to be 'a direct causal nexus between the act in question and the coercive effect.'[96] The change of policy, as one of the criteria for coercion, should be appreciated as any activity that would

89 Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction," *International Journal of Communication* 10 (2016). p. 4886.

90 Jamnejad and Wood, "The Principle of Non-Intervention." p. 371; Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace." p. 57.

91 Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace."

92 André Nollkaemper, *Kern van het internationaal publiekrecht*, *Boom Juridisch*, 8th ed (Den Haag: Boom juridisch, 2019). Bullet 321, p. 239. Nollkaemper argues, in the context of intervention, that 'it is undesirable to interpret the criterion of coercion too strictly'.

93 In fact, most non-forceful interventions are not obvious and therefore difficult to identify as coercive. Jamnejad and Wood, "The Principle of Non-Intervention." pp. 367- 377. The words 'particularly obvious' refer to the forceful interventions as mentioned in the Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

94 Case Concerning Armed Activities on the Territory of the Congo (DRC v Uganda) - Judgment, ICJ Reports (2005). Para 165, p. 227.

95 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 241, p. 124.

96 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 51.

change 'matters in which each State is permitted (...) to decide freely', due to the activities of the foreign State. This was certainly the case during the 2016 US presidential election.

Coercion remains to be an intentional act following from the rationale that a coercive intervention that fails to reach its goal is still coercive. The intent to act, or rather the intent to act coercively, irrespective of the changes it wants to achieve, remains pivotal to the notion of coercion.

To act coercively with the intention to undermine the control of the State applies to any situation in which pressure is used so the targeted State will be forced to change the decision it needs to make. Obviously, this could, on the one hand, be achieved by forcing a State to make a decision while under the threat of the use of force. On the other hand, it can be accomplished if the deliberate understanding and autonomous decision-making is circumvented altogether, which is the core characteristic of a manipulative influence operation (using covert and subconscious techniques).[97]

The complexity of cyberspace and the possibilities of its attributes call for a normative appreciation of coercion. That means normative in the sense that a line is drawn in the sand to indicate where coercive foreign infringements are accepted and where not. Reducing normative uncertainty benefits from a threshold for coercion that is not applied too strictly, hence that can easily be reached. The result of which is that States may take countermeasures to safeguard the line in the sand and legally protest against foreign infringement.

This means that coercion entails that a) the targeted State must have a deliberate intent to act in a coercive manner. The coercive manner means that b) the author State wants to undermine the deliberate understanding and autonomous decision-making of the targeted State, hence, to undermine State control. Finally, it means that c) the aim to change the policy of the targeted State must be interpreted in a negative manner. It is not required for the targeted State to have a clearly defined objective, which is a positive approach, but any deviation from the State activity of the targeted State would suffice.

If a manipulative influence operation has a deliberate intent to act and aims to change the existing policies of the target State, manipulative influence operations can be coercive, not least since undermining the deliberate understanding and autonomous decision-making process of the target State is the core attribute of manipulation.

97 See § 3.4.4.