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 6

CHAPTER 6: LEGAL ANALYSIS

This chapter contains a legal analysis of the operations set out in Chapters 4 and 5 and an assessment of the legal consequences of these operations. The results of this analysis are crucial in answering the 5th sub-question of this research: *"To what extent do activities of influence operations in the cases under discussion constitute a violation of sovereignty or non-intervention?"*

The crux of this research is not to determine whether or not the influence operations were successful in altering the results of the elections, but whether the influence operations, or the methods used, were in accordance with international law.[1] Though the thesis focusses on influence operations, hence soft-cyber operations, in the cases under discussion the hard-cyber operations are inextricably linked to the preparatory phase of the influence operations (during the 2016 US and 2017 French presidential elections). In assessing the legal consequences, the hard-cyber operations will therefore be taken into account.

This chapter starts with a brief outline of sovereignty and non-intervention in cyberspace particularly related to elections. The core of the chapter is the legal analysis of the RF influence activities during the 2016 UK EU referendum and the 2016 US and 2017 French presidential elections. Some key findings conclude the chapter.

Section 6.1.: The Legal Frame

'It is the effect of a cyber operation, not the target,
that usually determines whether a territorial sovereignty violation has been occurred'[2]

The legal foundation, and the conclusion of Chapter 3, is that respect for sovereignty and non-intervention is a binding rule of customary international law, which also applies in cyberspace. Violating these obligations means violating a primary rule of law which can, if the act is attributed to a State, constitute an internationally wrongful act. Both sovereignty and non-intervention are rules that apply solely in the relationship between States.[3]

1 Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018). p. 47.

2 Michael N. Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law," *Just Security*, 2021.

3 Terry D. Gill, "Non-Intervention in the Cyber Context," in *Peacetime Regime for State Activities in Cyberspace*, 2013, 217–38. p. 223; 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.

Foreign election interference may violate both the sovereignty of a State and the prohibition of intervention if the act is coercive by nature.[4]

6.1.1. Sovereignty

Sovereignty can be breached if the core elements of sovereignty, i.e. territorial integrity and political independence, are violated.

6.1.1.1. Territorial integrity

A breach of territorial integrity in the cyber context occurs when State A infringes on the territory of State B without the latter's consent and causes some form of (physical or functional) damage. The characteristics of activities in cyberspace complicate the applicability of these tenets. Since cyber-related activities very often physically cross borders, the actions are executed remotely from outside the State. Though damage may occur, most likely during hard-cyber operations, many cyber-related activities – especially soft-cyber influence operations are not intended to cause physical or functional damage.[5]

The domain for the violation of territorial integrity is the territory of the State including all persons and materiel, both public and private. Experts collaborating in the Tallinn Manual-process have indicated qualified thresholds for the nature of the breach of territorial integrity. This is not specific to influence operations, but to any (remotely executed) cyber-related activity.[6] A violation of the territorial domain occurs when 'certain effects of the cyber operation manifest themselves on the territory of the target state, whether on the government's cyberinfrastructure or that of private entities'.[7]

There is general agreement that if remote cyber-attacks cause physical damage or injury territorial integrity has been breached.[8] When (permanent) functional damage is the result of a cyberattack, territorial integrity could have been breached, but the experts might

4 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986). Para 205, p. 108; United Nations General Assembly, "Declaration on Non-Interference in the Internal Affairs of States - A/Res/31/91," 1976.; United Nations General Assembly, "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States - A/Res/36/103," 1981.

5 Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity (Forthcoming)*, 2019, 1–29. pp. 4-5.

6 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4(10), p. 20.

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

8 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 4(11), p. 20; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law."p. 43; Michael N. Schmitt, "Foreign Cyber Interference in Elections: An International Law Primer, Part II," *EJIL*, 2020. p. 1.

not agree on the specificities.[9] It is possible agreement could not be reached either on the threshold or on the specificities of effects in cyberspace below functional damage, such as the temporary loss of data or the slowing down of an ICT system. Activities, and above all their impact, below the threshold of functional damage could be unlawful depending on the context and require a case-by-case assessment.

6.1.1.2. Political independence

The political independence of a State is related to its inherently governmental functions. These State functions are generic and universal. Conducting elections or referenda are 'paradigmatic examples of an inherently governmental function',[10] and the *sine qua non* for democratic political systems to exist.[11] The same would hold for other inherently governmental functions, such as national defence, the tax collection or law enforcements tasks.[12]

Political independence is violated when the inherently governmental functions are violated. In the *Tallinn Manual 2.0* the nature of the violation is either interference or (more severe) usurpation.[13] Contrary to abusing territorial integrity, the violation of political independence does not require manifest effects (physical or functional damage) in cyberspace.[14] Interferences with inherently governmental functions have the intention to undermine, disturb or disrupt a State's ability to conduct its functions.[15] It is not required that the interference aims to change a certain policy of the target State or to take over the inherently governmental functions. Hence, activities with minor impact (including a DDoS attack on a governmental website or slowing down tax return software), which would otherwise (in the context of territorial integrity) fall below qualified thresholds of physical or functional damage, could suffice to violate State functions. Usurpation involves unilaterally taking

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

10 Steven J Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion," *Just Security*, 2017.; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 45.

11 Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion."; 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). p. 372.

12 But could also deal with related topics including legislation, social security or the national language. See: Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law."; Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," in *Cyber War: Law and Ethics for Virtual Conflicts*, 2015. p. 265.

13 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (10), p. 20; See also: Schmitt. para 16-17, p. 22; Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." p. 38.

14 Michael N. Schmitt, "Foreign Cyber Interference in Elections," *International Law Studies (Naval War College)* 97, no. 739 (2021). p. 753; 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. pp. 255.

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

over another State's inherently governmental functions and performing them without the injured State's consent.[16]

Meddling with elections may violate the sovereignty of a State via the notions of territorial integrity or political independence. Territorial integrity is violated when activities (in the context of foreign election influence) are executed within the targeted State without the latter's consent, or when damage is suffered due to (remote) cyber-related activity. On the other hand, political independence is violated if the nature of the activities amounts to a usurpation of, or interference with, the State function of holding elections or referenda.

6.1.2. Non-Intervention

An intervention is a coercive interference in the *domaine réservé* of another State. Cyber interference of a coercive nature may constitute a breach of the prohibition of intervention under international law.

The domain for a violation of non-intervention is the *domaine réservé* the area that is not governed by international legal obligations.[17] The *domaine réservé* encompasses 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely',[18] which includes jurisdiction over semi-public or private sectors.[19] A State's political system is a matter of internal concern.[20] National elections, therefore, fall within the reserved domain of a State.[21] A sovereign State is free to determine how elections are to be held, what

16 Schmitt. p. 45.

17 Schmitt, "Foreign Cyber Interference in Elections." p. 745.

18 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

19 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." pp. 7-8; Elements of the *domaine réservé* include the social security system, the fiscal system, fundamental operation of Parliament, or in the stability of financial system, or the legal system of a State. See: Przemysław Roguski, "Russian Cyber Attacks against Georgia, Public Attribution and Sovereignty in Cyberspace," *Just Security*, 2020.; Jeremy Wright, "Cyber and International Law in the 21st Century," 2018.; Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law* 42, no. 2 (2017): 1–21.

20 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. 36; Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention." p. 265, arguing that 'selection of a political system remains at the heart of sovereignty and, therefore, a core aspect of *domaine réservé*'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. para 205, pp. 107-108.

21 Steven Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion,'" *Duke Journal of Comparative and International Law* 30, no. 3 (2020). pp. 28-29; Ministry of Foreign Affairs, "Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace" (2019). p. 3; Michael N. Schmitt, "Foreign Cyber Interference in Elections: An International Law Primer, Part I," *EJIL*, 2020, 1–6. Other elements are e.g. the recognition of states and membership of international organisations; Schmitt, "Foreign Cyber Interference in Elections." pp. 745-746; 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. 318; 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. 49.

representative system is chosen, how its citizens participate and how the incumbents are elected, based on national jurisdiction.[22] Elections should be free from any form of foreign domination[23] or coercion.[24]

Coercion refers to 'pressure or compulsion that cannot reasonably be resisted',[25] entailing 'an affirmative act designed to deprive another State of its freedom of choice,[26] according to the *Tallinn Manual 2.0*. Coercion refers to the application of pressure,[27] compelling a State to adopt a decision regarding its policy or practice which it would not take as a free and sovereign State,[28] and must therefore be distinguished from persuasion, propaganda or public diplomacy.[29]

Coercion is the core element of unlawful intervention and, as put forth in Chapter 3, entails three elements.[30] The coercive State aspires to a) undermine the control and autonomous decision-making process of the target State,[31] b) do that in an intentional and deliberate way,[32] c) change the policies of that State or affect its behaviour 'with respect or a matter reserved for the target State',[33] *in casu* via the process of elections. It is irrelevant whether or not the attempted intervention was successful. An intervention that fails to reach its objective can still be considered a coercive intervention.[34] The fact that the injured State is

22 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 48-49; Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." pp. 8-9.

23 Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs." p. 37.

24 Chris Tenove et al., *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy, Centre for the Study of Democratic Institutions* (University of British Colombia, 2018). p. 9.

25 Dale Stephens, "Influence Operations & International Law," *Journal of Information Warfare* 19, no. 4 (2020): 1–16. p. 6; Henning Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law," *Israel Law Review* 53, no. May (2020): 189–224. p. 200.

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

27 Gill, "Non-Intervention in the Cyber Context." p. 223; Philip Kunig, "Prohibition of Intervention," *Max Planck Encyclopedia of Public International Law*, no. April (2008). Para 1; Maziar Jamnejad and Michael Wood, "The Principle of Non-Intervention," *Leiden Journal of International Law* 22, no. 2 (2009): 345–81. p. 348; Harriet Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention," 2019. p. 28; Antonios Tzanakopoulos, "The Right to Be Free from Economic Coercion," *Cambridge Journal of International and Comparative Law* 4, no. 3 (2015): 616–33. p. 620; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." pp. 200-202.

28 Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law*, 2013. p. 165; Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (Cambridge University Press, 2020). p. 80.

29 Jamnejad and Wood, "The Principle of Non-Intervention." p. 374; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (21) p. 318; Stephens, "Influence Operations & International Law." p. 7.

30 See § 3.3.4.2 & 3.4.3.2. See also: Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law." under Intervention; German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace," 2021. pp. 5-6.

31 Damrosch, "Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs." 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.

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

33 Schmitt. Rule 66 (19) p. 318.

34 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. 17.

not aware the intervention is taking place does not preclude its unlawful character,[35] nor is severity a determinative criterion for a coercive intervention. Both hard-cyber and influence (soft-cyber) operations can entail coercive aspects or amount to an operation that is coercive in nature.

Section 6.2.: The 2016 UK EU referendum

"A lie may be able to travel around the world before the truth has its shoes on, but an unchallenged untruth will never stop."[36]

On 23 June 2016, 51.9% of the UK voters chose to leave the EU. The result stunned many observers shortly after the referendum. Numerous academic studies followed that tried to explain the result and find the root causes of the UK sentiments towards the EU. Foreign influence activities during the election, especially from the RF, might also have to be factored in.[37]

During any election or referendum numerous domestic actors try to influence the registered voters. Canvassing, debating or campaigning activities are essential parts of the electoral process of a democratic political system, but these actions should be executed within an existing legal framework,[38] free from foreign interference.[39]

The main question in this section is whether RF influence operations during the UK EU referendum have violated the international rules of sovereignty or non-intervention.

6.2.1. Sovereignty

This section first discusses the possible violations of territorial integrity and, second, the political independence. Regarding territorial integrity, it is not documented that (while

35 Knowledge is relevant for seeking redress and invoking a wrongful act, but not for the breach of sovereignty itself.

36 Phil Williams, "Take the Time and Effort to Correct Misinformation," *Nature* 540, no. 7632 (2016).

37 House of Commons Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report," 2018. pp. 43-51.

38 The ICO is investigating allegations made about 'invisible processing' of people's personal data and the micro targeting of political adverts during the Brexit referendum. See: Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns," 2018.

39 Many States, including the UK and US, therefore have (or have passed) national legislation protecting the state against these influences e.g. cybersecurity acts, acts on prohibit foreign financial support to national elections. See: Intelligence and Security Committee of Parliament, Russia, 2020. pp. 33-37.

engaging in foreign influence operations) RF agents were active in the UK without the its consent. In that sense, there was not an unauthorised access to UK territory.

Contrary to the 2016 US, and the 2017 French, presidential elections the 2016 UK EU referendum did not experience a foreign intrusion into the election-related ICT systems, as far as is generally believed.[40] Nevertheless, apart from hard-cyber activities, the RF was engaged in soft-cyber influence operations during the run-up to the UK EU referendum.

The RF influence operation during the referendum contained elements of persuasive and manipulative influence activities. Leave camp politicians were supported by RF influence activities, including political grooming and supporting messages by way of the news outlets RT and Sputnik. The fact that the UK voters might not have been aware that RT and Sputnik were (biased) governmental outlets instead of independent news agencies strengthened the manipulative element in the influence operation. Moreover, manipulative acts by RF agents included the running of 419 Twitter accounts, pretending to be domestic actors, and the extensive use of bots. Due to these activities, the voters could not make a full appreciation of the available information.

The RF influence operations were executed from a distance and from outside the UK. The UK border was not physically crossed; therefore, the question is whether the influence operation violated territorial integrity based on the criteria set in the *Tallinn Manual 2.0*.

Fabricated content, misleading media sources and bots or information deluges due to political advertisements do not cause functional damage or the permanent loss of functionality[41] to (persons or materiel on) the territory of a State, or even physical damage or injury. Functional damage might entail the permanent disabling of ICT systems or the requirement to install new software packages. During the RF foreign election influence operation, no permanent functional impairments were documented. Not at any time in this case was it reported that data were deleted or altered which would indicate that there was no temporary loss of functionality either.

In sum, the activities of the RF influence operations during the 2016 UK EU referendum do not meet the criteria of violation of territorial integrity as stipulated in the *Tallinn Manual 2.0*. During the UK EU referendum RF agents did not take over State activities, hence the political independence of the UK was not violated due to usurpation of inherently governmental

40 Power outage was reported in some polling stations, but this could have been the result of the weather conditions on the day of the referendum, see: AFP, "UK Decides in EU Vote: Opinion Polls Put 'Remain' Camp Narrowly Ahead," *The Independent*, June 24, 2016.; Laura Galante and Ee Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *Atlantic Council* September (2018). p. 8. Galante suggests the option of a power outage, referring to Ciaran Martin, Chief of the UK National Cyber Security Centre who argues that RF have targeted UK's power supply on election day (in 2017). See: "UK Cyber-Defence Chief Accuses Russia of Hack Attacks," *BBC News*, November 15, 2017.

41 Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." pp. 38-39.

functions. However, RF cyber operations during the UK EU referendum did interfere with the inherently governmental function of conducting a referendum.[42] The question, however, is whether this interference was unlawful.

Given the fact that the interference did not require a manifest result,[43] that the effects of the interference were felt in the UK and that it was directed against the State or governmental functionalities[44] (a national referendum), it can be argued that the RF foreign influence operations could amount to unlawful interference. The RF influence operations 'disturb the territorial State's ability to perform the functions as it wishes'[45] thereby breaching the political independence of the UK and hence violating its sovereignty. The RF activities via social media, especially the use of bots and the running of Twitter accounts, influenced the public arena of the UK and extended beyond foreign propaganda. Official propaganda is an overt act, while numerous RF cyber-related activities were covert activities, and it is the covert nature of the activities that could qualify as unlawful interference.[46]

As a result, UK voters were hampered in their ability to voluntarily cast a free and deliberate vote; RF foreign influence operations could therefore be classified as unlawful interference with State functions of the UK.

6.2.2. Non-intervention

Infringements that are invasive into the reserved domain, whether traditional, via cyberspace or as influence operations, could amount to an intervention. The crucial question is whether the RF activities during the 2016 UK EU referendum were coercive.

Compelling influence operations may correspond with those for coercion. In most of the cases under discussion the influence operations are not compelling (forcing the other State to make an unwilling choice) but manipulative. The RF influence operation during the UK EU referendum was in part persuasive, but largely manipulative.[47] Persuasive influence

42 "The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means," Oxford Institute for Ethics, Law and Armed Conflict § (2020).

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

44 And not against purely commercial activities, see: Schmitt. p. 45.

45 Schmitt. p. 45.

46 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. 202. Denton analyses the so-called Facebook influence operation by RF and states that based on Schmitt covert actions could violate international law. See also: Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 46.

47 See § 5.2.1. on the operational analysis of the 2016 UK EU referendum.

operations, including overt expressions of propaganda or opinions opposing the policies of other States, are not unlawful.[48]

Manipulative influence operations that meet the criteria for coercion can still be coercive. To assess the coercive nature of the influence operations they are tested against the parameters of coercion referred to in Chapter 3. In other words, was the cyber-related activity intentional, did it undermine the deliberate understanding and autonomous decision-making, and did it have the aim to change the policy of the targeted State?[49]

The first criterion for coercion is the deliberate intent of the coercer to 'subordinate the sovereign will' of the target State.[50] The manipulative activities in UK case were intentional but do not appear to be pre-planned; they had an ad-lib and pragmatic character.[51] The RF influence operation was limited in scale. The core of the manipulative influence activities during the 2016 EU referendum was initiated (and prepared) by domestic (Leave camp) actors, with RF agents in support of the ongoing domestic (disinformation) campaigns, as their interests coalesced. The domestic actors were cognisant of the socially divisive topics in the UK as well as familiar with the ingrained preferences of certain groups, which could account for the fact that there was no need to steal data or hack the ICT systems of the relevant actors.

The second criterion is undermining the deliberate understanding and autonomous decision-making of the targeted State. Although the influence activities were only partially executed by RF agents and mainly by domestic actors, the RF did hamper the understanding and decision-making process. The RF influence operations induced a deflection into subconscious judgments by using deceitful and manipulative techniques, including bots, repetitive social media utterances and political advertising.

The last criterion for coercion is the aim to affect a change of policy of the targeted State, which is the core element of coercion. The influence operation during the 2016 UK EU referendum is primarily a domestic influence operation. Despite the fact that the domestic UK actors and the RF have different overall objectives for their respective influence operations, and the fact that the RF has a supportive role, the RF influence operation is coercive if it seeks to force 'the victim State to make different choices than it might were it free of coercive interference'.[52]

48 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 46.

49 See also: Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law." Under 'Intervention'; Barela related to hard-cyber operations, see: Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion.". See also § 3.5.2.

50 Jamnejad and Wood, "The Principle of Non-Intervention." p. 381; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 200.

51 Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 5; Dominic Cummings, "How the Brexit Referendum Was Won," *The Spectator*, 2017. See also section 4.2. of Chapter 4.

52 Duncan B. Hollis, "Russia and the DNC Hack : What Future for a Duty of Non-Intervention ?," *OpinioJuris*, 2016, 1–7.

Based on this rationale of the 1986 *Nicaragua* Case,[53] the RF influence operations are coercive in nature. In the Nicaragua Case the ICJ did not find it necessary to considered whether the US had the intent to overthrow the government of Nicaragua. The US support to the 'contras', who did have that aim, was sufficiently coercive.

Section 6.3.: The 2016 US presidential election

"When you have a massive propaganda effort to prevent people from thinking straight,
Because they're being flooded with false information and...every search engine,
Every site they go to, is repeating these fabrications, then yes,
It affects the thought process of voters".[54]

On 8 November 2016, Republican candidate Donald Trump was elected President of the United States of America (US). Election Day was preceded by an intense campaign between Trump and Democratic candidate Hillary Clinton. Already in the run-up to the election the US were made aware of possible RF influence operations and intrusions in the election infrastructure. After the elections several investigations on this topic commenced, such as the investigation into Russian interference by Special Counsel Robert S. Mueller.[55] The outcome of the investigation was that domestic legislation had been violated but the question remained whether the influence operation in this case also violated public international law related to the legal standards of non-intervention and the respect for national sovereignty.[56]

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

54 An apparent quote from the defeated 2016 Democratic presidential candidate Clinton, in Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (Random House, 2019). p. 210

55 Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," vol. I and II, 2019.

56 United States District Court, Indictment (United States v Andrienko) "Sandworm" (2020).; Information Commissioner's Office, "Monetary Penalty Notice" (2018).; United States District Court, Indictment (United States v Netyksho) (2018).; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 9.; Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 193-195; Darren L. Linvill et al., "'The Russians Are Hacking My Brain!' Investigating Russia's Internet Research Agency Twitter Tactics during the 2016 United States Presidential Campaign," *Computers in Human Behavior* 99, no. May (2019): 292–300. p. 292.

6.3.1. Sovereignty

To assess whether the sovereignty of the US was violated by the RF influence operation during the 2016 US presidential election an analysis of territorial integrity and of political independence was made. If either is breached, sovereignty is violated.[57]

Territorial integrity is violated when foreign agents operate from within the injured State without the latter's approval,[58] which was the case in the 2016 US presidential election.[59] RF agents had been in the US since 2014, initially to perform reconnaissance tasks.[60] Later on the RF agents in the US also engaged with US voters on social media, disguised as US virtual persona.[61] The RF also made use of terminals located in the US (Arizona) to relay data retrieved from the Clinton campaign team, DNC and DCCC ICT systems, to friendly systems,[62] most likely in the RF. The terminals in the US were operated remotely.

In the run-up to the 2016 US presidential election attempts were made, sometimes successfully, to hack the election infrastructure[63] and to scan data without damaging the physical network structure. Subsequently, RF agents gained access and most likely extracted 'data related to thousands of U.S. voters.'[64] As far as is known, no data were deleted or altered. In several cases the US-CERT[65] or the Department of Homeland Security detected the intrusion and blocked it.[66]

There is no indication that the intrusions into the election infrastructure caused physical damage or injury,[67] as referred to in the *Tallinn Manual 2.0* thresholds for the violation of territorial integrity via remote cyber operations.[68] Since the systems could operate

57 Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election." p. 371.

58 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 43.

59 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 21.

60 United States District Court, Indictment (United States v Internet Research Agency LLC) (2018). Items 4-5, p. 3.

61 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 22-24.

62 United States District Court, Indictment (United States v Netyksho), 1:18-215. Paras 8 & 24; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 38-39.

63 Renee Diresta et al., "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018. p. 4; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 2017. pp. 2-3.

64 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 50.

65 Computer Emergency Response Team, see: DHS & FBI, "Grizzly Steppe – Russian Malicious Cyber Activity," *Jar-16-20296*, 2016.

66 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. 12-20.

67 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 43.

68 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4(10), p. 20.

appropriately,[69] without an irreversible loss of function,[70] no argument can be found to state that (permanent) functional damage was inflicted on the ICT systems. Furthermore, given the fact that no data were deleted or altered, the breach might even fall below the lowest *Tallinn Manual 2.0* threshold of 'infringements falling below the threshold of loss of functionality'.[71]

Moreover, the *Tallinn Manual 2.0* experts agreed that if a State's cyber operations failed 'due to effective defensive measure or because the operation was flawed',[72] sovereignty is not violated. A rationale in line with the intrusion-based approach proposed by Roguski has it that unauthorised access as such would not amount to an intrusion, whereas deletion or alteration of data would.[73] The German position paper on the application of international law in cyberspace likewise argues that 'negligible physical effects and functional impairments below a certain threshold cannot (...) be deemed to constitute a violation of territorial sovereignty'.[74] A remote cross-border cyber-related operation scanning foreign ICT infrastructure without deleting or altering data, which could even be labelled as espionage, does not necessarily violate international law.[75]

Though numerous of these hard-cyber operations were attempted,[76] there was 'no damage or substantial loss of functionality to any cyber infrastructure' in the case of the 2016 US presidential election.[77]

The hack into the Clinton campaign team, the DCCC and DNC, differs from the intrusions on the electoral infrastructure or voting machines. Some, including Xiao or Hollis, suggest that the DNC hack did not violate sovereignty,[78] which might be true if one only considers the stealing of data. However, during the hacks into these institutions, malware (X-Agent) and backdoors (X-Tunnel) were installed. Though this does not amount to physical or functional

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

70 Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election." p. 371.

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

72 Schmitt. Rule 4 (24), p. 24.

73 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. Roguski's rationale is that not confidentiality or availability but violating the integrity of data is the crucial benchmark for an intrusion. See also Stephens, "Influence Operations & International Law." p. 8, arguing that destruction or manipulation of data, without (or irrespective of) the desire to coerce could amount a violation of sovereignty.

74 German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace." p. 4.

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

76 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." pp. 15-20.

77 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 47.

78 Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election." pp. 372-373; Duncan B. Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (2018): 31–46. p. 41.

damage, it could be concluded that the breaches aimed at the Clinton campaign team, the DCCC, and the DNC[79] were below the threshold of functional damage,[80] but above that of a *de minimis* violation.[81] Though it was not documented that data were altered or deleted, it is true that the RF agents put in malware and installed backdoors in the system, which are criteria also mentioned under the lowest threshold in the *Tallinn Manual 2.0*.[82] The infringement in this specific case would amount to a violation of sovereignty,[83] also according to Roguski's intrusion-based approach.[84]

Whilst RF executed a substantive social media campaign, especially in the 2016 US presidential election, the content that was posted did not damage the physical or functional architecture of private entities or enterprises such as Facebook.[85] The software used by SCL or Cambridge Analytica to gain access to data of the targeted audiences, , was designed to track persons, harvest their preferences and transfer platform (e.g. Facebook) users and their 'friends' to outside platforms. The applications used could have had a temporary impact on functionality of the ICT infrastructure of private companies in the US. However, the territorial integrity of the US is unlikely to have been violated due to the fact that applications were built by private entities and not by a foreign State or controlled or directed by a foreign State (i.e. the RF).[86]

The RF (soft-cyber) influence operations, executed during the 2016 US presidential election, were very often remotely operated activities and most RF agents conducting the influence operation did not physically cross any border. The manipulative influence operations, including disinformation and trolling campaigns but also the leaking of sensitive data from the Clinton and DNC hack, did not cause any physical or functional damage.[87] Moreover, the

79 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 38-40; Ido Kilovaty, "The Democratic National Committee Hack: Information as Interference," *Just Security*, 2016.

80 And though the *Tallinn Manual 2.0* experts could not agree 'to whether, and if so when' a cyber activity falls within this category, that does not mean that installing malware and backdoors as happened during the US case would not amount to this violation of territorial integrity. See: Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. rule 4 (14), p. 21.

81 Or violate national legislation, see: Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 193-195; United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32.

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

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

84 Roguski offers an alternative view to the sovereignty as a rule versus sovereignty as a principle discourse, by approaching the issue from a different angle. The penetration-approach argues that any intrusion is a violation of territorial integrity, while the 'de minimis'-approach generates room for interpretation. He seeks middle ground by proposing the intrusion-based approach. See: Przemysław Roguski, "Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views," *The Hague Program for Cyber Norms Policy*, 2020. pp. 4-7; Roguski, "Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach." pp. 77-80. See also 3.3.3.

85 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 201-202.

86 Data scientist Alexandr Kogan had developed applications to collect personal data which he (commercially) shared with Cambridge Analytica. Sponsored by the US republican Mercer, the data was used in the 2016 US elections, initially to support candidate Ted Cruz, see: James Ball, "The Real Story of Cambridge Analytica and Brexit," *The Spectator*, 2020.

87 Ohlin, *Election Interference: International Law and the Future of Democracy*. p. 73.

influence operation did not – contrary to the hack – penetrate any foreign ICT infrastructure. Data were not altered or deleted as a result of the influence operation.

In sum, the territorial integrity of the US was violated during the 2016 US presidential election, in the first place because RF agents were operating in the US without the latter's consent and, secondly, since malware was installed during the hacks into the Clinton campaign team, the DNC and DCCC, which would amount to an impairment of the ICT systems even though no actual physical or (permanent) functional damage occurred. The RF influence operation as such did not violate territorial integrity.[88]

State functions, or the inherently governmental functions of the State constitute the right domain for a violation of political independence. Contrary to the notion of territorial integrity, the State functions exclude purely private or commercial functions, even when executed by the State.[89] During the 2016 US presidential elections the RF did not take over or usurp inherently governmental functions, neither via hard-cyber hacks nor via influence operations. Whether the RF influence operation interfered with the US presidential election is another matter.

Changing the software of voting machines or altering the voting registration system would be a clear interference with a State function.[90] During the 2016 US presidential election the RF hard-cyber operations targeted the US election infrastructure. Though the election infrastructure could be defined as critical infrastructure in the election process, no software was changed during that operations. During the hack into the ICT infrastructure of the Clinton campaign team and the DNC, malware and backdoors were installed. On the one hand, it could be argued that the Clinton Campaign team and the DNC officially are private entities promoting specific interests,[91] and are therefore excluded from the remit of State functions. On the other, the DNC or DCCC are not considered as purely commercial. Moreover, as Tsagourias argues, 'interference should not necessarily target governmental functions; it can target any infrastructure, even a private one, provided that it is within a state's territory or jurisdiction'.[92] Besides, in a presidential campaign in a bipolar system such as the US the Democratic and Republican parties form the essence of the political ecosystem, The hack, especially when taking into account the subsequent release of the data that was retrieved

88 Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election." p. 371.

89 Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." p. 255.

90 Schmitt, "Foreign Cyber Interference in Elections." p. 753.

91 Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election." p. 361.

92 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. 6.

during (or as a result of) these hacks, therefore, amounts to interference with the political independence of the US.

The release of sensitive data – as part of the influence operation - stolen from the DNC and the Clinton campaign team, was surgically timed to interfere with the 2016 U.S. presidential election.[93] The release of mails, on 22 July 2016, just before the Democratic National Convention,[94] and the 7 October 2016 Access Hollywood-incident are examples of this.[95] If undermining the political process of holding elections as such was the target of the RF,[96] and perfectly in line with its strategic aim, it could amount to an interference with the inherently governmental functions since it directly relates to the State's ability to conduct elections.

Not all forms of cyber-related activities of influence operations interfere with the inherently governmental functions of another State. Election propaganda, diplomatic protest, purchasing political advertisements,[97] and criticising a foreign government in an international arena do not amount to violations of sovereignty.[98] Political propaganda campaigns and protests are accepted aspects of persuasive (foreign) influence operations.[99] A persuasive influence operation is not unlawful, but the dividing line between unwelcome propaganda and unlawful interference remains 'difficult to draw'.[100] Similarly, using social media platforms to overtly disseminate propaganda, even including fabricated information, is not unlawful per se.[101]

However, when a State uses covert tactics or subterfuge to propagate content – factual or fabricated – or impersonate US citizens,[102] mislead (African American) citizens in order to

93 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 36.

94 On 22 July 2016 some 20,000 email were release in which it became clear that the Democratic party favoured candidate Clinton over Sanders, while the DNC ought to stay neutral. On 26 July Clinton was still nominated as Democratic candidate, but DNC chairperson Wasserman Schultz was forced to resign. See: William Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0," *Texas Law Review* 95, no. 7 (2017): 1487–1513. pp. 1487-1488.

95 On 7 October 2016 candidate Trump receive negative publicity due to an interview published on the program Access Hollywood. Only hours later the information environment was surge with mail stolen from Clinton's chief of staff Podesta. The releasing of these mails quashed the previous scoop related to Trump. See: Ido Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information," *Harvard National Security Journal* 9 (2018): 146–79. pp. 156-157; Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019). pp. 120-121.

96 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." pp. 1-5.

97 Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election." p. 372.

98 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (29), p. 26.

99 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign."pp. 201-202; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 46; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

100 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." pp. 17-18.

101 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 46.

102 United States District Court, Indictment (United States v Netyksho), 1:18-215. p. 3. According to the indictment, the GRU agents used 'false identities and made false statements about their identities'.

dissuade them from casting their votes,[103] exploit fake or stolen identities as was the case during the 2016 US presidential election, it manipulates the ability of the US electorate to make a free and fair appreciation of the situation. This was the case during the 2016 US presidential election and, consequently, the RF undermined the public formulation of an independent opinion and subsequently the political choice.[104]

A single disinformation activity or the leaking of sensitive data as such might not affect the election,[105] which is underlined by Denton's conclusion that the social media-related RF influence operation 'fails to breach international law'.[106] Interference as a violation of political independence must be assessed on the specificities of the case. During the 2016 US presidential election, a wide variety of cyber-related activities were used during the influence operation. RF agents targeted the audiences in the US with fabricated content disseminated via deceitful media outlets. Moreover, the political advertisements and the leaking of sensitive data surged the public information environment with one-sided information, and the release of sensitive data was surgically timed. The result of this could be that the audiences in the US were invoked to side-line rational information processing and rely on biased judgment based on subconscious heuristics, since they could not give meaning to the overload of data, which was not fact-checked and whose origin was unknown. The inference as a result of the influence operation was furthermore exacerbated by the scandal surrounding the hard-cyber hacks into the Clinton campaign team, the DNC and the DCCC.[107] In turn, this could undermine the audience's ability to voluntarily cast a free and deliberate vote and could therefore amount to an unlawful interference with State functions.

All in all, the RF cyber operations in the run-up to the US presidential election interfered with the inherently governmental function of conducting elections.

103 Referring to the Blacktivist movement, which was set up by the IRA and not a domestic initiative, see: Filipe N. Ribeiro et al., "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook," *FAT* 2019 - Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency*, 2019, 140–49. pp. 142-143.

104 Judit Bayer et al., "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States," *Policy Department for Citizens' Rights and Constitutional Affairs*, 2019. p. 58; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 203; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 47.

105 Schmitt, "Foreign Cyber Interference in Elections." p. 754; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 47; Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 201-202. Denton argues that these social media based 'Facebook influence campaign' will violate domestic law but fail to breach international law.

106 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 202.

107 Shires argues that a hack can reveal sensitive data, but the hack as such could also create a scandal, see: James Shires, "The Simulation of Scandal : Hack-and-Leak Operations, the Gulf States, and U.S. Politics," *Texas National Security Review* Fall (2020). p. 15; Jeffrey Biller and Michael N. Schmitt, "Un-Caging the Bear ? A Case Study in Cyber Opinio Juris and Unintended Consequences," *EJIL*, 2018. p. 5.

6.3.2. Non-intervention

In this section, the question is whether the RF cyber influence campaign during the 2016 US presidential election as set out in Chapters 4 and 5 included conduct which may have constituted prohibited intervention. First, the hard-cyber operations supporting the preparatory phase of the influence operations will be analysed and, second, the (manipulative) influence operations.

In general, hard-cyber operations including falsifying election records or sabotaging voting tallies could qualify as coercive[108] because the targeted State is 'compelled to act in an involuntary manner or involuntarily refrain from acting in a particular way'.[109] Hacking electronic ballots would seriously undermine the ability of the State to conduct elections,[110] hence the State's choice of its political identity and organisation.[111] Schmitt argues that an infringement 'depriving a State to act vis-à-vis the *domaine réservé* are almost always coercive.'[112]

During the 2016 US presidential election, attempts were made to hack the election infrastructure including online voting systems and voter registration databases. The election-related infrastructure in at least 21 US states was accessed and voter's registration data might have been extracting, which would infringe the voting processes and democratic institutions.[113] In the end, records were not deleted or falsified, nor were the voting tallies sabotaged.[114] It is, however, unclear whether these attempts were cut short due to US vigilance,[115] or whether they were not intended to falsify records. Or as one of the US Officials during the investigation into the potential RF intrusion of the election infrastructure mentioned, they "didn't go in, but we don't know why",[116] drawing the analogy with a thief.

108 Aurel Sari, "Hybrid Threats and the Law: Concepts, Trends and Implications," 2020. p. 18; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 50; Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *Cambridge University Press*, 2013. Rule 10 (10), p. 47.

109 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (22), p. 24 & Rule 66 (21), p. 319.

110 The 2004 and 2014 Ukrainian presidential elections are examples of this sort of election fraud. In 2014 ultra-right candidate Yarosh was declared winner of the 2014 elections after a hack by the pro-RF CyberBerkut group, while in reality he had received 1% of the popular vote. See: Andreas Krieg and Jean-Marc Rickli, *Surrogate Warfare : The Transformation of War in the Twenty-First Century* (Washington, DC: Georgetown University Press, 2019). p. 100; Maksym Kovalov, "Electoral Manipulations and Fraud in Parliamentary Elections: The Case of Ukraine," *East European Politics and Societies* 28, no. 4 (2014): 781–807. pp. 783-784.

111 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (10) p. 315.

112 Schmitt, "Foreign Cyber Interference in Elections." p. 746.

113 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." pp. 22-32.

114 United States Senate Committee on Intelligence. p. 5.

115 United States Senate Committee on Intelligence. Chapter IV.

116 United States Senate Committee on Intelligence. p. 17.

Without doubt the US election infrastructure was scanned[117] and the DNC, the Clinton campaign team as well as the DNC and DCCC were hacked.[118] RF cyber-related activities were therefore deliberate which constitutes the first element of coercion. Given the strategic narrative of the RF (strong authoritarian systems prevail over feeble liberal democracies) and the bespoke frame stemming from that - to undermine the candidacy of Hillary Clinton - it can be argued that the intrusions also had the aim to change the policy of the US.

The notion of the change in policy would in this case mean that RF would support any candidate who running against Clinton, whether it be the Democrat Sanders during the Democratic primaries, the first Republican contender Cruz or, finally, Republican candidate Trump. This would highlight that the second criterion is fulfilled, though not all academics would agree. Hollis argues that 'there's little evidence that Russia was trying to coerce any particular result. Indeed, it is not even clear that the goal of the hack was to support Trump's candidacy."[119] Hollis argues that the RF could also have other goals for their influence operation including connecting it to the Panama case. Paradoxically, by stating that Hollis underlines that the operation certainly had the intent to force the US to change its attitude or behaviour, which is the essence of coercion.

The final criterion for undermining the ability and will of the State and its targeted audiences remains unsettled.[120] If, on the one hand, the hard-cyber action was merely aimed at scanning the elections infrastructure, it would not amount to coercion, since the ability of the targeted audiences (the voters) in the US to make autonomous decisions was not undermined due to the hack, and the US was still able to conduct elections. A computer intrusion as such does not compel the targeted audiences in the US to act in an involuntary manner,[121] or as Libicki states, related to the US case, 'the DNC hack was *not* vote-tampering'.[122] If, on the other hand, the aim was to falsify records or sabotage the voting machine, the operation was coercive even if it failed. Tampering the voting machines directly undermines the ability and will of the US voters to autonomously make decisions. The fact that the attempt was not successful does not preclude the coercive nature of the action.[123]

117 United States Senate Committee on Intelligence. pp. 10-21.

118 United States District Court, Indictment (United States v Netyksho), 1:18-215.

119 Hollis, "Russia and the DNC Hack : What Future for a Duty of Non-Intervention ?" p. 4.

120 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." p. 36.

121 Milanovic and Schmitt argue that the Russian hack of the Clinton team and subsequent release of data to Wikileaks did not amount to a coercion as it did not deprive the ability of the targeted State to act. See: Milanovic and Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic." pp. 269-270.

122 Martin Libicki, "The Coming of Cyber Espionage Norms," *International Conference on Cyber Conflict, CYCON* 2017-June (2017): 1–17. p. 6.

123 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (29) p. 322; Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 12.

Apart from the hard-cyber computer intrusions that took place in the preparatory phase of the 2016 US presidential election, the RF executed a sustained influence operation. In the run-up to 2016 US presidential election no (registered) threat was expressed that would amount to a compelling influence (soft-cyber) activity.[124] A compelling influence operation in this sense is an overt and conscious activity in which a clear threat (economic, informational or diplomatic) is expressed.[125]

The conclusion of Chapter 5 was that the cyber-related influence activities (including disinformation or trolling) were dominantly manipulative influence operations. Kilovaty would describe them as 'uncoercive methods – such as manipulation, deception, disruption, and disinformation - to trigger the involuntary actions of the victim state."[126] Manipulative influence operations make use of tools of influence that will invoke the reflexes towards heuristic manners of processing information i.e. limits in time, an overload of information and the subsequence inability to give meaning to the provided data.[127] The targeted audiences are often not aware of these covert and subconscious activities to lure them into biased judgments. Knowledge of the influence operation by the targeted State is, however, not a precondition for breaching the rule of non-intervention.[128] This means that covert activities could be qualified as activities amounting to unlawful interventions if the degree of manipulation is severe enough to eliminate the free will of the targeted audience.[129]

The cyber-related activities are dominantly, but not exclusively, manipulative influence operations; some persuasive influence operations did occur. Similar to the 2016 UK EU referendum, during the 2016 US presidential election RF agents purchased political ads on social media and shared news-topics via RT and Sputnik. These activities, when taken individually, are overt and persuasive influence activities. Despite the fact that persuasive influence activities can be intrusive in the reserved domain of a State, political advertisements, propaganda or critical (foreign) bloggers will probably not reach the threshold of coercion;[130] they are unwelcome rather than unlawful.[131] This assessment is aligned with the earlier

124 The use of compulsory cyber-power would be more affiliated with hard-cyber operations, see: David J. Betz and Tim Stevens, "Power and Cyberspace," *Adelphi Series* 51, no. 424 (2011): 35–54. pp. 45-46.

125 See § 2.2.4.

126 Ido Kilovaty, "The Elephant in the Room: Coercion," *AJIL Unbound* 113, no. June 27 (2019): 87–91. p. 88.

127 Buster Benson, "Cognitive Bias Cheat Sheet, Simplified," *Medium*, 2017.

128 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (25) p. 320.

129 Joseph S. Nye Jr., "Protecting Democracy in an Era of Cyber Information War," *Belfer Center*, 2019. p. 4.

130 Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, 2013. p. 201. Propaganda and could also be seen as the right to freedom of expression.

131 Wheatley, "Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about 'Coercion.'" p. 29 arguing that 'provision of factual information and commentaries on the news by foreign states, including by state-owned and state-controlled news media, does not violate the principle of non-intervention, no matter how unfriendly, or unwelcome.'; Schmitt, "Foreign Cyber Interference in Elections." p. 748.

conclusion that persuasive influence operations (foreign political propaganda or diplomatic protest) do not violate sovereignty based on the political independence of a State.[132]

This led Denton to provocatively argue that the influence operations via social media platforms including Facebook, fail 'to qualify as a violation of the norm of non-intervention'.[133] Hollis also argues that the RF influence operations do not violate the prohibition of intervention since in his definition of an influence operation, the 'goal of having a target adopt or change certain behaviors *willingly* (...) implies an absence of coercion"[134]. Hollis' definition aligns RF influence operations with persuasive influence operations in this thesis. Both Denton and Hollis refer mainly to the sharing of foreign political propaganda on social media platforms. Nonetheless, permitted foreign political propaganda has its limits. The 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States mentions that one of the duties of States is to abstain from 'any defamation campaign, vilification, or hostile propaganda'.[135] Foreign interference could transgress into activities that are coercive by nature or, as Egan stated: 'a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention."[136]

All this leaves the question when manipulative soft-cyber influence operations could be qualified as coercive.[137] The parameters of coercion will again be used as a tool to make an assessment, thereby taking the manipulative tenets related to the content of messages, the outlet of the content, and the overwhelming of the public sphere with one-sided information into account.

The RF influence operation in the run-up to the 2016 US presidential election must be regarded as a deliberate operation,[138] which constitutes the first aspect of a coercive act. Russian agents had been in the US since 2014, were actively engaged on social media platforms, and prepared numerous disinformation and trolling campaigns. Moreover, they

132 See supra § 6.3.1.

133 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 198.

134 Hollis, "The Influence of War; The War for Influence." p. 41.

135 United Nations General Assembly, "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States - A/Res/36/103." Under (j); Jamnejad and Wood, "The Principle of Non-Intervention." p. 374.

136 Brian Egan, "International Law and Stability in Cyberspace," *Berkeley Journal of International Law* 35, no. 1 (2016). p. 175.

137 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 200; Schmitt, "Foreign Cyber Interference in Elections." p. 750.

138 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." pp. 1-5; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 1-3; 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." pp. 35-37.

deliberately executed a campaign of leaking sensitive data obtained after the hack into the DNC, DCCC and the Clinton campaign team.[139]

Contrary to hard-cyber activities, the understanding and autonomous decision-making of the targeted audiences, the second criterion of coercion, was undermined by the RF manipulative influence operations. During these operations in the 2016 US presidential election fabricated or doctored content was shared via disinformation and trolling campaigns.[140], which increased or polarised socio-political divisions on topics such as race (BlackMatters)[141] and religion, but first and foremost undermined the integrity of candidate Clinton.[142] This was done to dissuade the targeted audiences from voting for Clinton.

Moreover, by using bots and mimicking US nationals,[143] RF agents were deceitful in the source of the content, in which case even 'factually correct information can be used as disinformation'.[144] Manipulating the outlets of content was further distorted by RT and Sputnik, which shared biased news while pretending to be independent news agencies. These impersonations prevented the voters from properly validating the authority of the data, thereby circumventing the voters' ability to understand or give meaning to the information received. The targeted audiences are lured into making biased judgments based on heuristics. The understanding and autonomous decision-making was further undermined by overexposure to one-sided information by leaking sensitive data and amplifying and repeating messages on a wide range of social media platforms. However, although releasing or purposely spreading disinformation or leaking sensitive data as such may 'influence votes, is not coercive because the voters still have the ability to vote as they wish'.[145]

All manipulative elements of influence activities related to the content, the outlet and the overload of one-sided information were activated during the 2016 US presidential election. In the US case the so-called Internet Research Agency (IRA)[146] 'created fake Facebook accounts

139 Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." Sections II & III; 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." Section IV.

140 Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 34 ff.

141 Philip N. Howard, John Kelly, and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project*, 2018. pp. 9-10.

142 Highlighting the killing of the Ambassador Stevens in Benghazi during her terms as Secretary of State, or linking her to a child trafficking network, see supra § 4.3.4.

143 Including fictitious persona such as 'Bertha Malone' or 'Helen Christopherson', United States District Court, Criminal Complaint (United States v Khusyaynova) (2018). Under C, Bullets 29-35.

144 Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 191.

145 Schmitt, "German Position on International Law in Cyberspace - Part I: General Interntional Law." Under 'intervention'; see also, Hollis and Neutze, "Defending Democracies via Cybernorms." p. 320.

146 The IRA, though a private entity operates as a proxy RF intelligence asset and was almost certainly tasked by the RF government to interfere with the US elections, 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. 5; United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32. pp. 2-11.

and purchased politically charged advertisements intending to influence the outcome of a U.S. election"[147] and, based on the rationale of the *Tallinn Manual 2.0*, mimicking domestic actors could even qualify as breaching the norm of non-intervention.[148] Schmitt argues that the 'covert nature of the troll operation deprived the American electorate of its freedom of choice'.[149] Moynihan asserts that 'coercive behaviour is perhaps best described as pressure applied by one state to deprive the target state of its free will in relation to the exercise of its sovereign rights in an attempt to compel an outcome in, or conduct with respect to, a matter reserved to the target state."[150] Due to the RF influence activities, US citizens could not value the information they received, which makes the covert activities manipulative and an example of psychological coercion.[151] Large numbers of voters were exposed to fabricated content via social media platforms, content that was often shared by RF actors masquerading as, or even pretending to be, US citizens, which impairs the voters' ability to understand the complex environment and, subsequently, to choose the candidate they prefer.

The final criterion for coercion is the aim to affect a change in policy. The political aim of RF influence operations as deduced in Chapter 2 is to create strategic confusion.[152] Creating confusion, with the purpose to undermine the perceived superior position of liberal democracies and to bring about increased respect for authoritarian regimes, is in line with sowing discord, which would be the effect of a disinformation campaign. This effect is intensified by the intent of a trolling campaign to polarise societies and increase socio-political divisions, and to undermine trust in State institution and the traditional media of the US. These manipulative techniques could amount to a change in policy. Policy in this sense does not need to be a very specific policy but can also mean a change in conduct or perception towards a subject.[153] In the US case, arguably the outcome the RF aspired to was to make sure Clinton would not be the next US President. Indeed, the frames the RF used during the 2016 US presidential election were aimed to denigrate candidate Clinton.

The essence of coercion is depriving the control of State B over its authority, free will and the ability to make free choices regarding its reserved domain,[154] such as elections or the formulation of foreign policy.[155] Following this description, and the three supportive elements of coercion as have been analysed above, it is fairly obvious that the RF manipulative

147 Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 199.

148 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 66 (10), p. 315.

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

150 Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention." p. 30.

151 Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 16.

152 See § 2.2.1.; Peter Pomerantsev, "To Unreality — and Beyond," *Journal of Design and Science*, no. 6 (2019).

153 Kunig, "Prohibition of Intervention." Under A.1.1.

154 Schmitt, "Foreign Cyber Interference in Elections." p. 746.

155 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Bullet 205, p. 108.

influence operations would amount to an intervention; a coercive interference in the reserved domain of the US.

Section 6.4.: The French presidential election

Retenez bien ceci Ferdinand,
ce que est le commencement de la fin de tout c'est le manqué de mesure![156]

On 7 May 2017 Emmanuel Macron won the French presidential election, at the expense of Marine Le Pen, with 66.1% of the votes in the second round. Macron and Len Pen had received most of their votes in the first round of the election on 23 April 2017. While traditionally the French political system alternates between left- and right-wing presidents, the 2017 presidential election differed.[157] The population appeared discontented with established political parties and politicians. The political parties therefore adopted more explicit political stances, including towards the EU or the RF. RF influence operations were, from the start, directed at supporting the pro-RF and antagonising pro-EU politicians, but the RF activities did not gain traction due to the lack of linguistic proficiency and cultural knowledge.[158] Macron's new political movement, the only pro-EU and anti-RF one, slowly gained prominence and, after the first round, became the main RF target.[159]

6.4.1. Sovereignty

This section discusses the violations of sovereignty by analysing the possible breaches of territorial integrity and political independence in the run-up to the 2017 presidential election. Though it was not documented that RF agents were active in France, they were during the RF presidential election. France itself has never attributed specific activities to the RF,[160] but certain sources claim to have evidence that the RF executed remote cyber-related operations

156 Louis-Ferdinand Céline, *Voyage a La Bout de La Nuit*, 1932. p. 534.

157 Jocelyn Evans and Gilles Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?," French Politics, Society, and Culture (Cham, Switzerland: Palgrave Macmillan, 2018). p. 1.

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

159 Jean Baptiste Jeangene Vilmer, "Lessons from the Macron Leaks," in *Hacks, Leaks and Disruptions*, ed. Nicu Popescu and Stanislav Secrieru, 2018.

160 "The Latest: France Says No Trace of Russian Hacking Macron," *AP News*, June 1, 2017.

from abroad.[161] The most prominent activity was the hack into the Macron campaign team, similar to the Clinton campaign team hack during the 2016 US presidential election.

The RF cyber-related intrusions did not breach the election infrastructure (related to the registration of voters or candidates, or the election-related ICT systems)[162] as far as we know, but they did hack the Macron campaign team.[163] Using methods of spear-phishing, the RF agents gained access to the Macron ICT systems via the email accounts of employees, which is similar to the approach used on the Clinton campaign team.[164] However, it is not known whether backdoors were installed in the ICT systems, as was the case with the Clinton campaign team, the DNC and the DCCC in the run-up to the 2016 US president elections.

The hack into the Macron campaign team did not cause physical nor functional damage. Following the thresholds of the *Tallinn Manual 2.0*, the hack into the Macron team could be considered a violation in the category below the threshold of functional damage.[165] During the hack no data were altered or deleted, nor were specific backdoors installed, but it was reported that a additional virtual drive was placed to gather data from the Macron ICT systems.[166] Though the hack into the Macron team was less severe than the hack into the Clinton campaign team or the DNC, DCCC, it could still amount to a violation of territorial integrity. This analysis is aligned with the intrusion-based approach,[167] arguing that scanning a port of a foreign computer, 'routing of cyber operations through foreign infrastructure [and] even gaining access to a computer network without proper authorization' would not violate territorial integrity.[168] Only when the integrity of the data (not the confidentiality or availability) is compromised (deletion or alteration of data, the implantation of malware, remote access) the interference with the functioning of ICT systems in the territory of another state, is territorial integrity violated. The territorial integrity of France was violated, not by the stealing of data from the Macron campaign team but by installing the ghost drive to retrieve data from the ICT system that was intruded on.

161 Including the companies FireEye, Microtrend and the US intelligence services, see: Dugald McConnell and Brian Todd, "French Presidential Candidate Macron Targeted by Hackers, Cyber Firm Says," *CNN*, 2017.; Thomas Brewster, "Did Russia Hack Macron? The Evidence Is Far From Conclusive," *Forbes*, May 2017.; Erik Brattberg and Tim Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks," 2018. p. 10; Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 12.

162 France was prepared and took measures to secure the infrastructure, including abandoning electronic voting, see: Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." pp. 9-10.

163 Jean Baptiste Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem" (Council, Atlantic, 2019). pp. 10-11;

164 Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 11.

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

166 Installing a ghost 'onedrive' or Microsoft storage website, to collect emails from the Macron campaign team, see: Feike Hacquebord, "Two Years of Pawn Storm," *Trendlabs Research Paper*, 2017. p. 13; Stefan Soesanto, "The Macron Leak That Wasn't," *European Council of Foreign Relations*, 2017.; Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." p. 9.

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

168 Roguski. p. 79.

On the one hand, the attributes of the soft-cyber influence operations during the 2017 French presidential election were focussed on trolling campaigns against Macron and the leaking of data from the Macron campaign team. On the other, the influence operation was only in part executed by RF agents. The activities of the influence operations during 2017 French presidential election, therefore, do not match the criteria of infringements of territorial integrity as stipulated in the *Tallinn Manual 2.0*. Fabricated content, misleading media sources or information deluges by leaking data cause neither physical damage or injury nor functional damage i.e. the permanent loss of functionality in the territory of a State.[169] Furthermore, the influence operations targeting the cognitive dimension by using cyberspace as a vector did not infringe the confidentiality, availability or integrity of ICT systems or the data they contain, therefore these operations also fall below the intrusion-based threshold since data were not deleted or altered.

Both foreign influence operations and hard-cyber operations that infringe the State's ability to hold national elections are invasive to the inherently governmental functions -the domain of political independence.[170] During the French presidential election in 2017, the RF did not take over State functions, neither with hard-cyber nor with soft-cyber activities.

The RF certainly interfered with the 2017 presidential election. By gaining access to the ICT systems, retrieving data and subsequently leaking these data the RF did not only interfere with the Macron team as a private entity, but also with the State functions of conducting elections. Whereas interfering with a private entity when, for instance, executing purely commercial activities might not amount to an unlawful interference with political independence,[171] interference while elections are being conducted would.

As mentioned in Chapter 4, due to the lack of an ongoing domestic influence operation in France, deficient understanding of French societal topics and preferences of the population, but also due to the futile spoils of the Macron hack**,** the influence operation was flawed. Moreover, the RF was not the only actor engaged in influence operations during the 2017 French presidential election; nor were they engaged in all the phases of the operation.[172] The influx of other entities, including the US alt-right and the French far-right,[173] was conducive to the disorganised and chaotic nature of the cyber-related activities.[174] Furthermore, the foreign influence campaign was impaired due to differences in institutional and legislative

169 Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law." pp. 38-39.

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

171 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." p. 47.

172 See § 4.4.7 & 4.5.

173 Emilio Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election," *First Monday* 22, no. 8 (2017). p. 1.

174 Soesanto, "The Macron Leak That Wasn't." p. 4; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 23-25.

domestic constellations,[175] such as 'the period of "election silence", the forty-four-hour media blackout just before the closing of the polls'.[176] In effect, it can be argued that the influence operation failed. Following the rationale of the *Tallinn Manual 2.0*-experts, a 'cyber operation that is designed to result in consequences breaching the sovereignty of another State fails for instance due to effective defensive measures or because the operation was flawed'.[177] In such a case sovereignty is not breached.

The analysis therefore is that the RF influence operation was an attempted interference in the political independence of France but failed to breach French sovereignty because the operation was flawed.

6.4.2. Non-intervention

The hack into the Macron team as well as the soft-cyber influence operations by the RF and other far-right entities during the presidential election took place in the reserved domain of France. To assess whether these invasive activities were coercive the three supporting tenets are used: undermine the control and autonomous decision-making process of the target State, act in an intentional and deliberate way, with the aim of changing the policies of that State.

Similar to the alleged manipulations during the 2016 US presidential elections, assessing whether the hack into the Macron campaign team undermined the control and autonomous decision-making process is difficult. The fact that the hack was flawed and did not 'produce the desired outcome has no bearing'[178] on this analysis because a coercive intervention that fails still breaches the prohibition of intervention. The hack might have affected the Macron team or its affiliates, but whether the hack as such undermined the audience's ability to voluntarily cast a free and deliberate vote is difficult to uphold. Moreover, the hack attempted on the 2017 French presidential election was not meant to falsify records or sabotage the voting machine.

While the Macron hack does not reach the threshold of the criterion related to undermining the control and autonomous decision-making process, it does reach the threshold of the

175 Structural reasons are the role of the Constitutional Council, the Media Regulatory Authority, the applicable EU General Data Protection Regulation of 27 April 2016, 2016/679 (applicable as of 28 May 2018), but also what Vilmer calls the robust media environment and the so-called Cartesians educational system ingrained with healthy scepticism. See Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 26-28; Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." pp. 8-9, see also: Chapter 4, sections 4.4.

176 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 12; Marie Baezner and Patrice Robin, "Cyber and Information Warfare in Elections in Europe," 2017. pp. 11-15.

177 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4 (24), p. 24.

178 Schmitt. Rule 66 (29), p. 322.

other two. The Macron campaign team was hacked. Several researchers have pinpointed the RF affiliated APT 28, or Fancy Bear, as the main actor involved.[179] Based on metadata the preparatory activities may well have started a year before the actual hack.[180] The hack was, therefore, deliberate and intentional.

The Macron hack would also fit in the RF narrative to undermine the EU coherency and sow distrust in liberal democracies. The RF did not have a specific candidate they would support, but the aim to change the policy in France was meant to support those candidates that were pro-RF and anti-EU. Early in the elections a range of Eurosceptic candidates from the far-left (Mélenchon) to the far-right (Le Pen) could be distinguished.[181] Cyber-related activities crystallised later in the campaign, especially after the first round, with the aim to support Le Pen and antagonise the pro-EU candidate Macron.

The parameters of coercion will also be used to assess whether these manipulative influence activities were coercive by nature. There is a deliberate intent to execute the influence operation, if only to exploit the data retrieved from the Macron hack. The case differs from the influence operation after the 2016 hack on the Clinton campaign team. The lack of sensitive materiel obtained from the hack could have induced the RF to cancel the influence operation or at least to deprioritise it, after which non-aligned domestic far-right and US alt-right agents may have taken over the initiative.[182]

In the run-up to the 2017 French presidential election the RF has manipulated the content of messages via disinformation but mostly trolling operations, depicting Macron as an aristocratic Marie Antoinette,[183] a spy or a homosexual,[184] which was content picked up by far-right entities and occasionally traditional media. For the RF, using media outlets to destabilise the French voters was more challenging now that RT and Sputnik had been uncovered as an RF governmental outlet.[185] Interestingly, the data retrieved from the Macron hack was doctored with before dissemination, which undermined the authenticity of the content.[186] Due to the potentially early cancellation of the influence operation the RF were not, or not fully, engaged in the phase of exploiting social media to repeat and magnify

179 Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 12.

180 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 19.

181 Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." p. 10.

182 But, activities that cannot be attributed to States (or in specific cases International Organisation) do not fall within the remit of non-intervention, see Gill, "Non-Intervention in the Cyber Context." p. 223.

183 DFRLab, "'Macron Antoinette': Alt-Right Targets France," *Atlantic Council*, 2017.

184 Nathalie Raulin, "Macron Gay? L'intéressé Se Marre," *Liberation*, February 7, 2017.; Sputnik News, "Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests," *Sputnik*, February 4, 2017.

185 Jean-Philippe Louis, "Face à Vladimir Poutine , Emmanuel Macron Tacle Les Médias Russes RT et Sputnik," *Les Echos*, May 29, 2017.

186 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 14.

content so that the French public information environment was not surged with one-sided data.

The influence operation might still have had the aim to bring about a change of policy,[187] in the sense that the RF wanted a pro-RF and anti-EU candidate to become President of France, similar to the analysis made for the coercive nature of the Macron hack.

All in all, the influence operation by the RF during the French presidential election might have had an initial intent to coerce but the RF did not pursue the operation, leaving it manipulative by nature and not coercive.

Section 6.5.: Key Findings

> *Although there is nothing necessarily new about propaganda, the affordances of social networking technologies—algorithms, automation, and big data—change the scale, scope, and precision of how information is transmitted in the digital age.*[188]

The key findings provide an answer to the third sub-question: *'To what extent do activities of influence operations in the cases under discussion constitute a violation of sovereignty or non-intervention?'* (SQ3).

Election is a core element related to sovereignty and non-intervention of the State. Conducting elections and referenda are a State function (related to sovereignty). They also fall within the reserved domain of the State (related to non-intervention), or as Corn argues, '(t)he quintessential example of a violation of the principle of non-intervention is one state coercively interfering in the internal political process of another state, such as by altering the votes recorded and thereby affecting the results of an election.'[189]

In the cases under discussion both hard-cyber (ICT intrusions and hack) and soft-cyber influence activities were executed. Influence operations that use cyberspace as a vector with the aim to target the cognitive dimension were used in all three cases. To support the

187 Jamnejad and Wood, "The Principle of Non-Intervention." p. 348; Wheatley, "Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber." p. 8.

188 Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation," 2019. p. 11.

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

preparation of influence operations, hard-cyber activities were employed during the 2016 US presidential election[190] and the 2017 French presidential election.

6.5.1. The 2016 UK EU referendum

During the 2016 UK EU referendum it was not documented that there was a physical presence of RF agents in the UK without official authorisation. Furthermore, no hard-cyber operations were witnessed in the preparation of the RF influence operation.

As the UK border was not physically crossed the RF influence operation during the 2016 UK EU referendum was executed remotely and from outside the UK. The activities of the RF influence operations in this case i.e. using fabricated content, misleading media sources, using bots or information deluges by way of political advertisements, do not reach the criteria as stipulated in the *Tallinn Manual 2.0*. Since these activities did not cause physical, functional or other damage, the territorial integrity was not violated by the remote influence operation.

No usurpation of State functions occurred during the 2016 UK EU referendum. The political independence, however, was violated because of unlawful interference with State functions of the UK. RF activities via social media, especially the covert use of bots and the running of Twitter account influenced the public arena of the UK to such extent that they hampered the voters in their ability to voluntarily cast a free and deliberate vote.

The influence operation during the 2016 UK EU referendum was mainly a domestic operation by the Leave camp. Though the supporting RF influence operations were mainly manipulative activities, they would amount to coercion because they sought to find manners to lure the UK voters into making decisions they might otherwise not make. The RF influence operations were pre-planned, but they had a clear intent to deliberately engage in the UK EU referendum and support ongoing domestic (disinformation) campaigns. The understanding and decision-making process was also interfered with by using deceitful and manipulative techniques including bots, repetitive social media utterances and political advertising. Though the role of the RF was limited, the RF influence operation was coercive in the sense that it supported domestic actors that had the aim to change the policy of the UK.

In short, although territorial integrity was not breached, the RF influence operations subverted the sovereignty by breaching the political independence and violated the prohibition of intervention.

190 Office of the Director of National Intelligence, "Foreign Threats to the 2020 US Federal Elections," 2021. p. 1; Schmitt, "Foreign Cyber Interference in Elections." p. 740.

6.5.2. The 2016 US presidential election

During the 2016 US presidential election the sovereignty of the US was impinged upon by a breach of its territorial integrity and political independence.

The territorial integrity was attacked, first by RF agents who were on US territory without permission and, second, by way of the installation of malware on the Clinton campaign team, the DNC and DCCC ICT infrastructure. Neither the scanning of the ICT election infrastructure, nor the RF influence operations, amounted to a violation of US territorial integrity. To all intents and purposes, the soft-cyber influence operation did not violate territorial integrity.

Similar to the UK EU referendum, no usurpation was documented during the 2016 US presidential election. US political independence was, however, compromised due to the unlawful interference with the inherently governmental function of conducting elections. The RF influence operation undermined the US public's formation of an independent opinion and, subsequently, its political choice by using covert tactics, impersonating US citizens, or exploiting fake or stolen identities.

Regarding the prohibition of intervention, given the data available it cannot be concluded that the hacks into the election infrastructure, but also into the Clinton campaign team, the DNC and DCC, were coercive. Whether these hacks undermined the control and autonomous decision-making process of the US voters remains undecided.

The soft-cyber influence operation, however, amounted to a coercive intervention. The essence of coercion is depriving the control of State B over its authority, free will and the ability to make free choices regarding its reserved domain,[191] such as organising elections or formulating its foreign policy.[192] The influence operations were deliberate actions that undermined the understanding and autonomous decision-making of the targeted audiences in the US. During the election fabricated content was shared via disinformation and trolling campaigns with the aim to increase or polarise socio-political divisions. RF agents also used bots and mimicked US nationals. Finally, the influence operation was aimed to affect a change in policy, making sure that candidate Clinton would not be the next US president.
In short, the influence operations violated sovereignty by causing a breach of the political independence and transgressing against the principle of non-intervention. The territorial integrity of the US was violated during the RF activities, but not via soft-cyber influence operations.

191 Schmitt, "Foreign Cyber Interference in Elections." p. 746.

192 Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports. Para 205, p. 108.

6.5.3. The 2017 French presidential election

The hack into the Macron campaign team during the 2017 French presidential election indeed violated the territorial integrity of France, not by the stealing of data from the Macron campaign team but by installing the ghost drive ('onedrive') to retrieve data from the ICT system that was intruded.

The activities of the influence operations during 2017 French presidential election did not match the criteria for infringement of territorial integrity as stipulated in the *Tallinn Manual 2.0*. Fabricated content, misleading media sources or information deluges by leaking data caused neither physical damage or injury, nor functional damage. Furthermore, the influence operations did not infringe upon the confidentiality, availability or integrity of ICT system since data were not deleted or altered during the soft-cyber influence operation that was only in part executed by RF agents.

In line with the UK and US cases, no usurpation of inherently governmental functions took place during the 2017 French presidential election. The hack into the Macron team, however, could be considered an unlawful interference, in a similar fashion as the hack into the Clinton campaign team in the 2016 US presidential election, since the hack had the intent (and effect) to disturb the State function of conducting elections. The soft-cyber operation did not amount to the unlawful interference with political independence. The influence operation was flawed, in which case sovereignty is not breached.

Regarding non-intervention, the intrusion into the ICT system of the Macron campaign team does not constitute an intervention per se.[193] Though, assuming that the hack was planned, with a deliberate intention to gain access to the ICT systems, the hack as such (not the subsequent leaking of sensitive data) lacked the (coercive) element of undermining the decision-making process of the targeted audiences.[194]

Likewise, the soft-cyber influence operation did not amount to coercive intervention. Though the influence operation was a deliberate activity, using a hack to gain sensitive data that could be leaked, the failure of obtaining any data did not provide the RF with instruments to undermine the understanding and autonomous decision-making of the targeted audiences. It could even be argued that the RF disengaged from influencing French politics after the failed hack into the Macron team. Changing the policy of France might still have been the initial aim of the RF influence operation. All in all, the influence operation by the RF during

193 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law ?," *Texas Law Review* 95 (2017): 1579–98. p. 1592; Hollis, "Russia and the DNC Hack : What Future for a Duty of Non-Intervention ?"

194 The Manual's experts were split as to whether such cyber operation would violate the norm on non-intervention, indicating that the law is unsettled and lacks granularity on the scope of prohibited cyber intervention.

the French presidential election contained elements of manipulative influence operation, but it was not coercive.

In short, as was the case in the 2016 UK EU referendum and the 2016 US presidential election, the RF influence operation in France did not breach territorial integrity. While in the other cases sovereignty was violated based on political independence, this is not what happened. French sovereignty was violated, but this was due a breach of territorial integrity resulting from the hack into the Macron campaign team. No intervention occurred during the RF influence operation at the time of the 2017 French presidential election.