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 5

CHAPTER 5: OPERATIONAL ANALYSIS

During the 2016 EU referendum in the UK, and during the 2016 US and 2017 French presidential elections, as examined in Chapter 4, foreign agents executed influence operations. The so-called Mueller report on the RF interference during the 2016 US presidential election found that the RF government carried out a sustained campaign to interfere in the election, undermine trust in democracy, and provoke and amplify political and social discord, which reached over 100 million US citizens online.[1]

In this chapter an operational analysis is made on what sort of influence has been exerted during the three influence operations set out in Chapters 4. The analysis of the cases is based on the operational framework (the key findings of Chapter 2) and will provide an answer to the 4th sub-question: *How do the mechanisms of influence apply to the influence activities in the cases under discussion?*

First, a brief recapitulation of the mechanisms of influence, related to persuasion, compellence and manipulation. The core of the chapter is an analysis on how the mechanisms of influence are applied during the cases under discussion. The chapter concludes with several key findings.

Section 5.1.: Mechanisms of Influence

"It has to happen without thinking"[2]

Cyberspace is part of the information environment and, for the purpose of this thesis, entails the virtual dimension and the physical network layer of the physical dimension. Cyber operations can target the layers *in* cyberspace – hard-cyber operations - but can also use them as a vector (*via* cyberspace) to affect the cognitive dimension. The latter are soft-cyber operations.

1 Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," vol. I and II, 2019. pp 4-7; Jamie M. Fly and Laura Rosenberger, "The Mueller Report Shows Politicians Must Unite to Fight Election Interference," *Foreign Affairs*, 2019, 1–7.

2 An alleged quote by Cambridge Analytica CEO Alexander Nix referring to the psychographic 'propaganda' the firm was disseminating, in: Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Harper, 2019). p. 326.

Cyber-related influence operations are inherently soft-cyber activities that use cyberspace as a vector (targeting the cognitive dimension) with the aim to alter the deliberate understanding and autonomous decision making of targeted audiences in another State – State B. The academic difference between hard- and soft-cyber operations does not preclude that soft-cyber influence operations may be supported by hard-cyber operations, or that hard- and soft-cyber operations coalesce, for instance during hack-and-leak operations.[3]

To achieve its main aim of altering the deliberate understanding and autonomous decision making of targeted audiences, influence operations will utilise persuasive, compelling or manipulative forms of influence. Hard-cyber operations, or hacks, can be compelling but are, in the context of this research, not defined as influence operations.

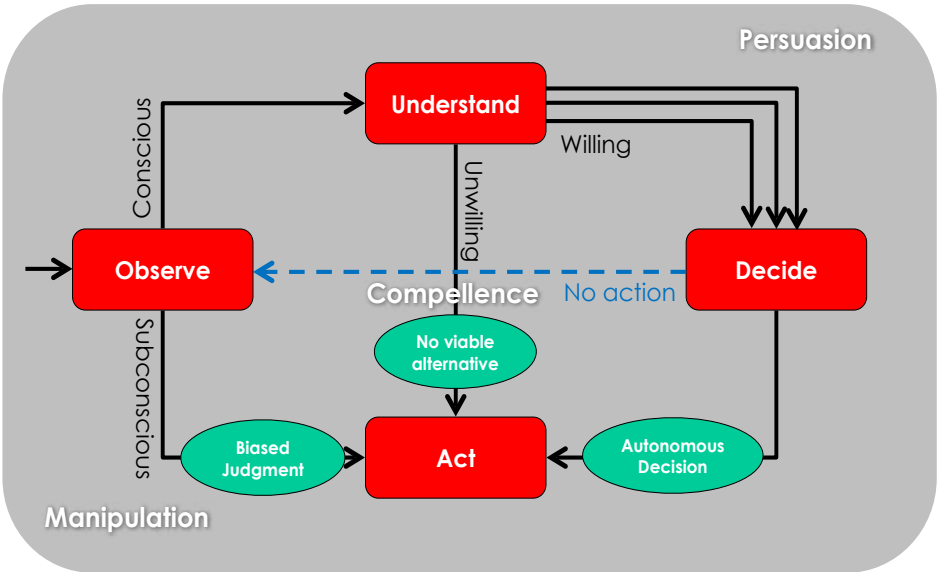

Figure 5- 1 Forms of Influence Operations

Persuasive influence operations aim to alter the perception and understanding of target State B and, consequently, the weighing of the options to choose from. Persuasive influence operations try to influence the targeted audiences overtly,[4] in a conscious way, during which the targeted audiences of State B are still able to make an autonomous decision i.e. a voluntary (willing) and meaningful choice based on the options available. Keeping in mind

3 James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," *Journal of Cyber Policy* 4, no. 2 (2019): 235–56. pp. 236-238.

4 Such as Radio Free Europe/ Radio Liberty, incepted in 1949.

Nye's notion of soft power, a persuasive influence operation reflects the 'ability to get what you want through attraction and persuasion rather than coercion or payment'.[5] Expressing verbal criticism within the perimeters of how a State conducts an election, including lobbying, propaganda or broadcasting during those foreign elections, is not in itself compelling since the voters, and therefore the target State, are not forced to make an unwilling choice.[6] In this sense, Stephens would qualify persuasive influence activities as a form of diplomacy, while foreign interferences make use of clandestine and deceptive methods.[7]

Compelling influence operations, similar to persuasive influence operations, make use of overt and conscious techniques with the aim to limit the decision-making options available to, the targeted audience leaving them no meaningful alternatives to choose from. Compelling influence activities short-cut or circumvent the deliberate understanding and autonomous decision-making process of the targeted audiences of State B forcing them to consciously make an unwilling choice and change of policy,[8] subsequently.

Whilst persuasive and compelling influence operations make use of conscious techniques, manipulative influence operations use subconscious techniques to subvert or usurp the autonomous decision-making process. Manipulative influence operations lure targeted audiences into making reflexive biased judgments based on cognitive and social heuristics. Manipulative influence operations are mostly covert and therefore do not change the weighing of the options to choose from but circumvent the deliberate understanding and autonomous decision making of the targeted State altogether. In other words, the targeted audiences are not forced but are duped into making choices that are not autonomous.

The manners of influence are the main levers shaping the frames that operationalise the strategic narratives of the assertive State – State A. Frames that highlight socially divisive topics are more rational and conscious by nature, seeking to start a dialogue within a society.[9] The more the frames rely on and incorporate the ingrained preferences - social and cognitive subconscious heuristics - of the targeted audiences, the more manipulative

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

6 Terry D. Gill, "Non-Intervention in the Cyber Context," in *Peacetime Regime for State Activities in Cyberspace*, 2013, 217–38. p. 223; 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. pp. 6 & 39-40; Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," in *Cyber War: Law and Ethics for Virtual Conflicts*, 2015. p. 261; Quincy Wright, "Subversive Intervention," *The American Journal of International Law* 54, no. 3 (1960): 521–35. pp. 530-531 mirroring the argument, stating that propaganda is at a non-State level, protected by the freedom of opinion and expression, unless it is intended to incite aggression.

7 Dale Stephens, "Influence Operations & International Law," *Journal of Information Warfare* 19, no. 4 (2020): 1–16. p. 15; though the division between the two remains subtle, see: Maziar Jamnejad and Michael Wood, "The Principle of Non-Intervention," *Leiden Journal of International Law* 22, no. 2 (2009): 345–81. pp. 374-375.

8 Steven Wheatley, "Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention," *EJIL*, 2020.

9 See § 2.2.2. & § 2.2.4.

they are. Manipulative influence operation cut short or bypass deliberate understanding and autonomous decision making, which may lead to biased or manipulative judgments. The heuristics of targeted audiences cannot be manipulated as such since there are cognitive reflexes. Manipulative influence operations will therefore use tools to invoke the subconscious processing of information resulting in a biased judgment. The lack of time to make a decision, an overload of information and consequently the inability to give meaning to the provided data, are tools to lure audiences into making biased judgments based on heuristic side-lining of the rational, conscious decision-making process.

Section 5.2.: Operational Analysis of the Cases

The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country.[10]

In general, influence operations follow a sequence of preparation, execution and exploitation. In the cases under discussion, not all RF influence operations followed this sequence, as was described in Chapter 4. In the run-up to the 2016 US presidential election and the 2017 French presidential election, hacking attempts were made during the preparation of the influence operation. While during the 2016 UK EU referendum, it appears that the RF influence operation had an ad-lib character supporting the execution and exploitation phase of an on-going domestic influence operation. In the 2017 French case, the RF influence operation lost momentum after the hack into the campaign team of candidate Emmanuel Macron did not yield any sensitive materiel.

Engaging with the target audiences and therefore influencing these audiences commences with cyber-related activities, which include disinformation and trolling campaigns. The cyber-related activities during the 2016 UK EU referendum, the US presidential election and the 2017 French presidential election aimed to undermine public trust in State institutions and the electoral system and aggravate the socio-political difference.[11] In the cases under discussion, the targeted audiences were not only influenced by doctored content (e.g. via disinformation and trolling campaigns), but the content was also presented through deceitful outlets. RF agents operated regular social media accounts impersonating domestic

10 Edwards L. Bernays, *Propaganda*, 2nd Print (New York: Horace Liveright, 1928). p. 9.

11 United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," 2018. pp. 121-124; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 4.

(US or UK) actors.[12] Also, the biased government-led news agencies, such as RT or Sputnik, pretended to be independent news outlets.[13]

Influence activities related to content and the outlet of messages are intensified by the overwhelming vastness of information in the digital domain. The RF executed and exploited influence activities on Facebook, Twitter, RT and Sputnik,[14] in order to overwhelm audiences with (a variety of) data and information. The inundation was intensified by one-sided political ads, leaking of sensitive data and excessive repetition of messages. The 'information deluge',[15] generated by foreign political advertisements, leaking of information and amplifying messages may result in a rapid information flow giving the targeted audience 'little time to process and evaluate new information'.[16] While the leaking of data as such – especially if they are factual data – is not unlawful,[17] the dissemination of large volumes of one-sided information is cognitively disorienting and possibly confusing. Without alternative and counterbalancing sources of information, the ability of the targeted audiences to consciously and rationally process information (even if it is propaganda) is deflected towards the subconscious way of processing information, based on heuristics and ingrained preferences. In that sense, the 'electorate's freedom of choice was being thwarted'.[18]

Foreign political grooming is a supportive activity which includes purchasing political advertisements, providing funds to political parties to buy airtime. Political grooming exacerbates the provision of one-sided information to a targeted audience.[19]

Amplifying messages make use of the 'computational propaganda'[20] i.e. the suggested relationship between activities and occurrences based on algorithms generate correlations that are not based on causality. Moreover, the characteristics of cyberspace facilitate

12 Savvas Zannettou et al., "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web," *Arxiv*, 2019. p. 9; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 14-15.

13 United States Department of State, "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem," 2020. p. 3.

14 Ilya Yablokov, "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)," *Politics* 35, no. 3–4 (2015): 301–15. p. 312.

15 Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity (Forthcoming)*, 2019, 1–29. p. 18.

16 Lin and Kerr. p. 18.

17 Referring to the rules on non-intervention in international law, see: 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). p. 29.

18 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. 51.

19 See also: Jamnejad and Wood, "The Principle of Non-Intervention." pp. 368-369; Jens David Ohlin, "Election Interference: The Real Harm and The Only Solution," *Cornell Law School Research Paper No 18-50*, no. 50 (2018).

20 Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction," *International Journal of Communication* 10 (2016). p. 5;

the exploitation of social media platforms, including by using bots or 'fake' social media accounts to surges of biased information.[21] Combining the automation with a degree of human interaction will 'help avoid detection and make interactions feel more genuine'.[22]

The effect is manipulative if the abundance of one-sided content dominates the information environment of the audiences and the audiences are no longer able to make up their own minds. The question that arises is whether these attempts to influence or deceive the targeted audiences were persuasive, manipulative or compelling?

5.2.1. The 2016 UK EU referendum

During the 2016 EU UK referendum the RF influence activities were limited, in comparison to the 2016 US presidential election. The influence activities were mainly prepared and executed by domestic actors i.e. the (Vote) Leave and Remain camps.

As far as has been documented, there was no hack into the ICT systems of political actors or parties, nor was there a hack on the voting infrastructure by a foreign entity during the 2016 UK EU referendum. The data that were needed to generate frames, to craft cyber-related activities such as the disinformation campaign and micro-target the UK audiences, were obtained by domestic actors (Cambridge Analytica/ AIQ) via web-based applications generating personal data taken form Facebook accounts.

During the UK EU referendum, the disinformation campaign was largely initiated by domestic actors.[23] The RF (soft-cyber) influence activities were focused on supporting the on-going domestic influence campaigns - via trolling activities and on exploiting social media in order to amplify and magnify the existing cyber-related activities. In the UK case, media outlets RT and Sputnik published 261 articles with an anti-EU sentiment.[24] The news outlets RT and Sputnik were initially presented as independent news agencies broadcasting in the English language. Russian news outlets, including RT and Sputnik were also active in supporting the leader of the UK Independence Party and other Leave camp politicians. RF

21 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. p. 39.

22 Samantha Bradshaw and Philip N. Howard, "Troops, Trools and Troublemakers:A Global Inventory of Organised Social Media Manipulation," *Computational Propaganda Research Project*, vol. 12, 2017. pp. 11-12.

23 Sascha O Becker, Thiemo Fetzer, and Dennis Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis," *Economic Policy* 32, no. 92 (2017): 601–51. pp. 613-615. See also § 4.2.4. and 4.4.4.

24 House of Commons Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report," 2018. Para 162; 89 up, "Putin's Brexit? The Influence of Kremlin Media & Bots during the 2016 UK EU Referendum," 2018. Slide 8; Laura Galante and Ee Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *Atlantic Council* September (2018). p. 9.

agents also allegedly facilitated broadcasting and conveying political messages for the Leave camp.[25]

UK citizens could have been deceived if they were not (or could not have been) aware of the true identity and affiliation of these news agencies. Supporting foreign candidates via news outlets could be an act of propaganda, a manner to persuade a target audience, including in another State. However, hiding behind a false identity or hiding the true affiliations of an outlet as the RF did with RT and Sputnik is a covert act which is manipulative in nature. The RF also acted manipulatively when the Internet Research Agency (IRA)[26] was running 419 so-called 'false front'[27] Twitter accounts to circulate messages highlighting social discord with the focus on anti-Muslim texts or echoing and retweeting messages with a 'Leave-related' context.[28] Here, too, the UK citizens' ability to assess the validity of the incoming data was undermined.

The UK case also saw multiple 'bots', used by the RF to support and amplify statements of Brexiteers (Leave camp). These software programmes were used to take over repetitive human actions and amplify the content. The average UK voters could not validate the authenticity of the messages sent by these bots which, on face-value, appeared to be UK citizens. Howard and Kollanyi argue that '(i)t is no secret that citizens, journalists, and political leaders now make use of political bots—automated scripts that produce content and mimic real users. But it is not clear that average users can distinguish bot from human activity'.[29] The bots, especially stemming from foreign entities, could invoke subconscious heuristics based on the conformity, authority and familiarity bias[30] and thereby manipulate UK voters. The messages forwarded by bots during national elections would be valued differently if the voters knew that they originated from a foreign agent. Here, again, the elections were disturbed since, due to the deceitful outlet and the overwhelming volume of one-sided data, the voters could not make a full appreciation of the available information.

25 Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." p. 14.

26 The IRA is a private enterprise that almost certainly operates as a proxy for and has been tasked by RF intelligence agencies. 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; Richard Sakwa, "Russo-British Relations in the Age of Brexit," 2018. p. 26.

27 Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 9.

28 Vidya Narayanan et al., "Russian Involvement and Junk News during Brexit," *Comprop Data Memo 2017.10*, 2017. p. 2; Yuriy Gorodnichenko, Tho Pham, and Oleksandr Talavera, "Social Media, Sentiment and Public Opinions: Evidence From #Brexit and #Uselection," *National Bureau of Economic Research*, 2018. p. 23.

29 Philip N. Howard and Bence Kollanyi, "Bots, # StrongerIn, and # Brexit: Computational Propaganda during the UK-EU Referendum," *Comprop Research Note 2016.1*, 2016. p. 5.

30 Johan E. Korteling, Maaijke Duistermaat, and Alexander Toet, "Subconscious Manipulation in Psychological Warfare," 2018. pp. 16-17 & 25.

5.2.2. The 2016 US presidential election

RF agents, active during the 2016 US presidential election, had been in the US at least since 2014. They had been active in executing influence operations from within the US but mainly from abroad – often the RF, in case of the IRA activities. The RF prepared, executed and exploited a State-led influence operation to change or undermine the US presidential election with the aim to sow social discord, undermine trust in the government and media and to exacerbate divisions.[31]

The RF activities during the run-up to the elections were broader than solely cyber-related influence operations. The activities included the setting up of an administrative base for all election-related matters,[32] and associating with specific US agencies or organisations including the National Rifle Association.[33] Moreover, a prominent RF activity during the preparatory phase was hacking into several US-based ICT systems.

During the 2016 US presidential election attempts were made to hack the election infrastructure including online voting systems and voter registration databases.[34] In more than twenty US States RF agents attempted to scan data, gain unauthorised access to voting related repositories or websites.[35] In a few US States these attempts were successful and the RF could engage in scanning activities, but in other cases they merely 'knocked on the door'.[36] In the end, based on the data available, there were 'no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted.[37] In some cases, the intrusion was discovered, and additional measures were taken to stop it.[38] In the end there is no evidence that any of these attempts was successful. Neither

31 United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 3.

32 Mrs Khusyaynova was charged for running or supporting the so-called Project Lakhta, the administrative base for election-related RF activities in the US. See: United States District Court, Criminal Complaint (United States v Khusyaynova) (2018).; United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 43.

33 United States Senate Committee on Foreign Relations, "Minority Report on Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." pp. 51-52.

34 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 2017. pp. 2-3; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 50-51; 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. 22 ff; Renee Diresta et al., "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018. p. 4.

35 United States District Court, Indictment (United States v Netyksho) (2018). p. 25. The GRU agents obtained information 'related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers'.

36 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. 20. RF activities were related to penetrated voter registration database, viewed multiple database tables, and accessed voter registration records.

37 United States Senate Committee on Intelligence. p. 38.

38 United States Senate Committee on Intelligence. pp. 15-20.

the election infrastructure nor voter registration data were destroyed or manipulated, which meant that the physical network structure was not corrupted.[39]

Hack, or intrusions into the ICT infrastructure, also occurred to support the preparation of the soft-cyber influence operation. Apart from the intrusion into the electoral infrastructure, the Clinton campaign team, the DCCC and DNC were also hacked. The hacks into the Clinton campaign team, DNC or DCCC during the 2016 US presidential election, were deliberate activities to violate the privacy of personnel of the Democratic Party, pilfer data and install malware in the ICT network.

As mentioned earlier, the methods of influence are related to soft-cyber influence operations and not to hard-cyber hack operations, which does not take away the compelling or deterring nature of a hard-cyber operation. Hacking, both into the US electoral infrastructure and the Democratic campaign entities, could have compelling effects. By hacking an ICT system and stealing or copying data, the US might have been forced to act, to install new software, to replace computers,[40] or to decide to vote manually.[41] When sensitive data are stolen, the owner of the data could after conscious deliberation be forced to brief the general public pro-actively in case the stolen data are released, or he might even be forced to step down, which influences the domestic political process of elections. The fact that the victims do not have alternative options to choose from makes the act compelling.[42]

The RF influence operation during the 2016 US presidential election used techniques related to doctoring the content, the outlet and the volume of the data made available. Fabricated content was shared via disinformation and trolling operations. Disinformation was shared extensively during the US presidential elections of 2016. The IRA sent bespoke messages to Patriots ('Being Patriotic'), LGBT, Muslim Americans ('United Muslims for America') and their opposition ('Stop Islamization of Texas'),[43] with the intention to manipulate or radicalise their behaviour and create or foment division along racial, religious and political fault lines.[44] The IRA not only fuelled sentiments revolving around existing organisations such as the Tea Party or Black Lives Matter, but also created new allegedly grassroot initiatives including the 'Blacktivists', 'BM' or 'BlackMatters' with a focus on African-American cultural

39 Also in the French case There were no hard-cyber operations directed at election infrastructure since France has abandoned nearly all electronic (or on-line) voting.

40 As was the case during the so-called 2012 Saudi Aramco hack. See e.g. Harriet Moynihan, "The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention," 2019. p. 21.

41 The Netherlands have decided to vote manually based on threat of being hacked, see: Marie Baezner and Patrice Robin, "Cyber and Information Warfare in Elections in Europe," 2017. p. 14.

42 Wheatley, "Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention."

43 Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 19-20.

44 Ritam Dutt, Ashok Deb, and Emilio Ferrara, "'Senator, We Sell Ads': Analysis of the 2016 Russian Facebook Ads Campaign," in *ICIIT 2018*, ed. L. Akoglu, vol. 2 (Springer Singapore, 2019), 98–112. p. 166.

and racial issues and police brutality.[45] These initiatives are deceptive and manipulative since they invoke the association principle, making audiences accept the initiatives without scrutiny. The association principle lies at the basis of the heuristic of pattern recognition i.e. seeing coherent structures in 'an abundance of information'.[46]

The trolling and defamation activities in the US case were principally directed at candidate Clinton. She was defamed as a person, not as a political figure, and associated with child trafficking ('pizzagate'),[47] selling weapons to ISIS, and the 2012 killing of US Ambassador Stevens in Benghazi,[48] with the purpose to undermine her integrity and reputation.[49]

Disinformation as such is not prohibited.[50] Sharing factual information with other States, or influencing them with it, is accepted, which, however, does not mean that disseminating fabricated information is unlawful per se.[51] The disinformation campaign as such could be regarded as a persuasive influence operation and continuation of US political warfare or, in this case, the RF Active Measures doctrine. Transgressing into trolling and defamation would make them more manipulative since a trolling campaign relies on subconscious heuristics and emotions of groups within societies, rather than on socially divisive topics.

Apart from using fabricated data during the 2016 US presidential election RF agents manipulated social media accounts and created virtual persona (social media identities),[52] posing as Americans, or even impersonating actual Americans (which included the fictitious social media persona 'Jenna Abrams', 'Helen Christopherson' and 'Rachel Edison').[53] By

45 United States District Court, Indictment (United States v Internet Research Agency LLC) (2018). pp. 14-15; Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 9-10; Alicia Parlapiano and Jasmine C. Lee, "The Propaganda Tools Used by Russians to Influence the 2016 Election," *The New York Times*, February 18, 2018.

46 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 12.

47 Pizzagate refers to an incident in December 2016, when an armed gunman, inspired by conspiracy theories stemming from Reddit, 4Chan, and InfoWars, entered a local pizza joint in Washington, DC, to check out an alleged secret paedophilia dungeon reportedly run by Bill and Hillary Clinton in a Pizza restaurant. Before being arrested, the gunman fires three shots into the restaurant, without hitting someone. See: Samantha Korta, "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security," *Homeland Security Affairs*, no. March (2018). p. 9. Marc Fisher, John W. Cox, and Peter Herman, "Pizzagate: From Rumor, to Hashtag, to Gunfire in D.C.," *The Washington Post*, December 6, 2016.

48 Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 12-14.

49 United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 3.

50 Björnstjern Baade, "Fake News and International Law," *European Journal of International Law* 29, no. 4 (2018): 1357–76. pp. 1362-1365. Baade makes the difference between a false news, which could violate the rule of non-intervention only if a number of other criteria are fulfilled, and distorted news which will – in general – not violate the rule of non-intervention.

51 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. 18.

52 On platform such as Facebook, YouTube, Twitter, Tumblr and Instagram. 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." Para VII, pp. 43-62.

53 Yiping Xia et al., "Disinformation, Performed: Self-Presentation of a Russian IRA Account on Twitter," *Information Communication and Society* 22, no. 11 (2019): 1646–64. pp. 1649 ff. Ohlin, "Election Interference: The Real Harm and The Only

impersonating US citizens, RF agents were 'feigning the true source of the disinformation'.[54] Using these techniques is deceptive. The target audience is unaware that their ability to formulate a voluntary choice is being undermined via 'mechanism involved impersonation of U.S. citizens through social media to amplify particular social and political positions'.[55] Some of these RF IRA-affiliated actors even worked from within the US[56] in order to accentuate divisive US political and social topics or induce grassroot initiatives related to Tea Party activists, Black Lives Matter or immigration.[57] The fictitious US virtual persona were also used to promote and whitewash sensitive information that had been leaked.[58] Executing cyber-related activities and exploiting them using fake identities undermines the process of making a free choice. The targeted audiences could not value the information they received, which render covert activities manipulative, and examples of psychological coercion.[59]

IRA agents also used other techniques to mask or camouflage their identities.[60] The virtual identity Guccifer 2.0 allegedly was a Romanian hacker responsible for the DNC hack.[61] However, these forms of concealing an identity are less intrusive and deceptive than pretending to be a fellow-national: US voters will be suspicious of any non-native outlet, whether of RF, Romanian or Latvian descent.[62]

Furthermore, the IRA purchased some 3,500 ads referring to divisive and inflammatory social issues regarding race, sexuality, gender identity, immigration and Second Amendment,[63] which were also used to organise rallies to support Trump ('Trump is our only hope for a

Solution." pp.5-6; United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 5; Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 46-47; 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'; United States District Court, Criminal Complaint (United States v Khusyaynova), 1:18-464. Bullets 39-42.

54 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." pp. 46-47.

55 Ohlin, "Election Interference: The Real Harm and The Only Solution." p. 7.

56 Their presence in the US was as such not per se a violation of international or national law, see: United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32. p. 13.

57 Diresta et al., "The Tactics & Tropes of the Internet Research Agency." On IRA tactics, pp. 34 ff.

58 United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 13-14. The GRU unit 74455 supported unit 26165 during the publication of the stolen data.

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

60 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. 296.

61 Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, D.C.: Georgetown University Press, 2020). p. 78; United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 14-15.

62 Korteling, Duistermaat, and Toet, "Subconscious Manipulation in Psychological Warfare." p. 25.

63 The Second Amendment was a 1791 addition to the US Constitution and protects the right to keep and bear arms. See also: United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 45.

better future!') or to oppose Clinton ('Hillary Clinton Doesn't Deserve the Black Vote').[64] Another example of the IRA overwhelming the US information environment with one-sided data is the leaking of sensitive data. During the US case genuine (but confidential) documents from the DNC, the DCCC, and the email account of John Podesta, chairman of Hillary Clinton's 2016 presidential campaign, were leaked,[65] causing considerable impact during the Democratic Congress.

Finally, the RF also exploited social media by repeating and amplifying messages. The RF agents operated not only one platform but executed a wide plethora of cross-platform activities[66] in order to magnify the content of disinformation campaigns.[67] By constantly repeating these often false and fabricated messages they become familiar, and in the end were perceived to be true, which may serve as an illustration of the productive power of cyberspace.[68]

Similar to the UK case, political advertisements in the US case could be regarded as a form of persuasion. The trolling campaign, or the act of impersonating US citizens are manipulative by nature. Both manipulative activities aim to circumvent the deliberate understanding and autonomous decision-making process of the US voters, luring them into making biased judgments. The leaking of sensitive data could even compel a political figure to make an unwilling choice, as happened to the DNC chairperson, Debbie Wasserman Schultz.[69] Though these compelling activities indeed influence a political person, they do not necessarily influence the targeted audience.

Combining all elements of the soft-cyber influence operation by the RF to influence the 2016 presidential elections, it can be argued that the campaign was in essence largely manipulative. The RF, who were active from the preparation to the exploitation of the influence operation, used techniques that included mimicking US citizens on-line, overwhelming the US information environment with one-sided data that eroded Clinton's position (and advanced Trump's), with intense trolling and defamation campaigns against Clinton, and sensitive data leakages which undermined Clinton's candidacy even further.

64 United States Senate Committee on Intelligence. pp. 7-11, 40, 44; 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. 189.

65 United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 5; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 41-49.

66 Including Twitter, Instagram, YouTube, Facebook, Reddit, Tumblr, and to a lesser extent LinkedIn, Medium, Pinterest and Google, see also Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 189 ff.

67 Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 8-11; Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 14-15.

68 David J. Betz and Tim Stevens, "Power and Cyberspace," *Adelphi Series* 51, no. 424 (2011): 35–54. pp. 50-53.

69 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.p. 149; Jonathan Martin and Alan Rappeport, "Debbie Wasserman Schultz to Resign D.N.C. Post," *The New York Times*, July 24, 2016.

The RF influence operation meddled with the content, source and volume of the information that the US audiences received. This may have induced their inability to accept or make sense of the data available, which in turn invoked social and cognitive heuristics instead of processing data based on rationality.

5.2.3. The 2017 French presidential election

The RF activities during the French presidential elections of 2017 took place at the start of the election campaigns. The hack into the campaign team of candidate Emmanuel Macron can be attributed to agents affiliated to the RF,[70] but although the activities that followed are pro-Russia, they are most likely not initiated or controlled by the RF. These were potentially individual actions by US alt-right and French far-right activists.

The most prominent cyber-related influence activity during the French 2017 election was the leaking of information concerning candidate Macron, which had been preceded by an intrusion into the ICT systems of the Macron campaign team.[71] The hack was deliberate and intentional, and though the intruders did not damage the ICT system or delete data, they certainly installed malware to monitor and retrieve data connected with Macron's campaign team. Though the yield of the hack was futile, the Macron team decided to report the hack and make it public. Given the content of the stolen data (which included Macron's personal university notes)[72] it is difficult to uphold that Macron was forced to make the decision to inform the public.[73]

The RF cyber-related influence activities during the 2017 French elections were mainly focussed on trolling and leaking of undisclosed data. During the elections the disinformation campaign was largely absent,[74] contrary to the trolling and defamation activities that were directed against Macron at the time. The RF outlets Sputnik-France and RT-France, which were active at this stage,[75] suggested that Macron was a US agent, an Islam protagonist, and

70 Erik Brattberg and Tim Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks," 2018. pp. 9-11.

71 Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019). pp. 360-361; United States District Court, Indictment (United States v Andrienko) "Sandworm" (2020). pp. 15-16.

72 Stefan Soesanto, "The Macron Leak That Wasn't," *European Council of Foreign Relations*, 2017.

73 Baezner and Robin, "Cyber and Information Warfare in Elections in Europe." p. 15.

74 Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." pp. 613-615; Jean Baptiste Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem" (Council, Atlantic, 2019). 26-29. See also § 4.2.4. and 4.4.4.

75 Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." pp. 10-11.

had questionable sexual morals.[76] The trolling campaign was manipulative by nature since it tried to invoke the emotions and ingrained preferences of the French voters.

Apart from influencing the audiences by meddling with content and outlet of the content, the RF influence operations could have flooded the information sphere with political advertisements. In the French case, however, the foreign political support was directed at providing loans to parties rather than at purchasing airtime,[77] hence it had no cyber-related impact.

Leaking of sensitive data could also have contributed to the information deluge. By overwhelming the targeted audience with large quantities of information whilst they are given little time to digest it, the rational understanding and decision-making process is paralysed and clogged,[78] and judgement is deflected towards heuristics. During the 2017 French presidential election documents were shared via the #MacronGate hashtag on the US-based 4chan platform and, in a later phase, another set of data ('MacronLeaks') from the Macron campaign team was leaked to the press.[79] To create plausible deniability the RF agents suggested that the initial data leak from the Macron campaign team stemmed from a Latvian IP address.[80] This attempt may have obscured the originator of the leak, but did not have a deceitful effect on the French voters. Neither Russian nor Latvian originators invoked the familiarity bias, leaving the targeted audiences sceptical. Before the leaks were released numerous documents had been doctored with, combining a disinformation and a leaking campaign. In a general sense, the sharing of stolen data is already manipulative, since the voters are unable to validate the authority of the data provided. Fabricating data that are about to be leaked, however, is manipulative both in content and in the source of the content.

Overall, the RF influence operation during the 2017 French presidential elections was impaired. The RF tried to influence the public debate in France, at first via Sputnik News and RT.[81] However, contrary to the 2016 UK EU referendum, during the French elections in 2017, RT and Sputnik were exposed as RF controlled outlets, or 'agents of influence',[82] rendering

76 Jean Baptiste Jeangene Vilmer, "Lessons from the Macron Leaks," in *Hacks, Leaks and Disruptions*, ed. Nicu Popescu and Stanislav Secrieru, 2018. p. 76; Sputnik News, "Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests," *Sputnik*, February 4, 2017.

77 Jocelyn Evans and Gilles Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?," French Politics, Society, and Culture (Cham, Switzerland: Palgrave Macmillan, 2018). p. 100; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 24-25.

78 Daniel Kahneman, *Thinking, Fast and Slow* (London [etc: Penguin, 2012). pp. 36-37.

79 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 4.

80 Chris Doman, "MacronLeaks – A Timeline of Events," AT&T Alien Lab, 2017, https://cybersecurity.att.com/blogs/labs-research/macronleaks-a-timeline-of-events. Using the 4chan political board: http://boards.4chan.org/pol/thread/123933076 (no longer on-line)

81 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 4-6.

82 Mona Elswah and Philip N. Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)," *Journal of Communication* 70, no. 5 (2020): 623–45. p. 623; Jean-Philippe Louis, "Face à Vladimir Poutine , Emmanuel Macron

the manipulative impact less effective. Moreover, shortly after the leaks, the Macron team came forward and announced that the leaked documents contained 'deliberately forged (...) and proactively planted false information'.[83] Furthermore, during the French case, the content that was shared by RF agents was mainly written in the English language, which triggered French reluctance, not due to the content but to the obviously foreign origin of the content.[84]

Some content was repeated and magnified via Twitter but also via RF news outlets RT and Sputnik, albeit to a much lesser extent. The reason for this lack of manipulative intent could be that there was a declining RF interest in the elections due to the unsuccessful hack and its problematic adaptation to French language and culture.

Section 5.3.: Key Findings

"Social media and its widespread adoption have changed the nature and practice of human interaction for much of the world."[85]

The key findings prompt an answer to the 4th sub-question: *How do the mechanisms of influence apply to the influence activities in the cases under discussion?*

Influence operations can make use of persuasive, compelling or manipulative mechanisms to influence the targeted audiences. This is not a categorical division, since in reality an influence operation might use several frames to operationalise the strategic narrative, which may combine these mechanisms of influence.

In general, preparation of (soft-cyber) influence operations i.e. formulating the intent, narrative and the frames stemming from the narratives, can be finalised without interacting with foreign entities; no engagement with other States is therefore required.[86] The large quantities of data and the analysis of these data required during the preparation, can be acquired via data scientists, long-term country surveys or the services of consulting agencies

Tacle Les Médias Russes RT et Sputnik," *Les Echos*, May 29, 2017.

83 Boris Toucas, "The Macron Leaks : The Defeat of Informational Warfare," *CSIS Briefs*, 2017., p. 2.

84 Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 29.

85 United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media." p. 8.

86 Contrary to the 2016 US presidential election, the 2020 election did not witness any 'attempt to alter the technical aspect of the voting process', see Office of the Director of National Intelligence, "Foreign Threats to the 2020 US Federal Elections," 2021. p. 1.

(Cambridge Analytica, Aggregate IQ).[87] It is also possible to obtain sensitive data by hacking into the ICT computer systems of the (foreign) targeted audiences.[88] However, if a State decides to make such an intrusion (hack) into the ICT systems, it will engage with other States.

During the case under discussion both hard-cyber (hacking into ICT systems) and soft-cyber operations (influence operations using cyberspace) were witnessed. During the 2016 US presidential and 2017 French presidential election hard-cyber operations, including intrusions into a foreign (electoral) ICT system, were executed to support the preparation of the influence operation. Though hard-cyber activities (including hacks) are not influence activities as defined in this thesis, they may still have a compelling nature and also violate the international law standards of sovereignty or non-intervention, as will be explained in Chapter 6.

The (soft-cyber) influence operations in the cases under discussion were predominantly manipulative influence operations. Though persuasive activities could be detected,[89] especially regarding RT and Sputnik broadcasts, or the purchase of political advertisements which can be regarded as a form of foreign political propaganda. The lion's share of the RF cyber-related activities was neither persuasive nor compelling but covert and deceptive instead.

The manipulative mechanisms used to stimulate subconscious ways of processing information are connected to the content of messages, the outlet of the content and the inundation of the public sphere with one-sided information. The influence operations in the cases discussed were deceitful since their content during the disinformation campaigns was fabricated or doctored aiming to sow discord and, by means of trolling campaigns, exacerbating the socio-political divisions and polarisation of societies.

By using bots and mimicking nationals (e.g. US citizens) the RF agents were deceitful in the source of the content, i.e. how the content was shared. Biased information was disseminated by agencies including RT and Sputnik. This is manipulative since the outlet appeared to be independent news agencies while they were RF-aligned actors. The impersonations of their countrymen prevented the US voters from genuinely validating the authority of the data, thereby preventing them from making a deliberate verification of the information.

87 Which in turn make/made use of large sets of data from Facebook. See for instance: Carole Cadwalladr, "Exposing Cambridge Analytica: 'It's Been Exhausting, Exhilarating, and Slightly Terrifying,'" *The Guardian*, September 29, 2018.

88 Feike Hacquebord, "Two Years of Pawn Storm," *Trendlabs Research Paper*, 2017. pp. 4-7.

89 Though outside of the virtual dimension, the meetings between the Trump campaign team and envoys from RF president Putin on the future US-RF relationship, and revisiting the sanctions regime on RF would therefore rather be examples of persuasive influence, see: Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 159-160.

Finally, the information deluge caused by foreign political advertisements, the leakage of sensitive information and the amplification and repetition of messages on a wide range of social media platforms, resulted in a rapid information flow of one-sided information.

In sum, the cyber-related influence activities in the cases under discussion were predominantly manipulative in origin. The speed and overload of information, combined with the covert nature of the influence activities, and hence the inability to validate the content, force the targeted audiences to deflect towards reflexive responses and biased judgments based on ingrained preferences and heuristics, rather than relying on conscious and rational appreciations. Manipulating the content, outlet and flooding the information environment with one-sided biased data is advantageous to obstruct the deliberate understanding and autonomous decision making of the targeted audience.