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

Link to publication

Citation for published version (APA):
Pijpers, B. M. J. (2022). *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*. [Thesis, fully internal, Universiteit van Amsterdam].

Chapter 4

CHAPTER 4: ON INFLUENCE OPERATIONS – the CASES

In Chapter 2 a concept was provided explaining how State A can execute operations via cyberspace to influence the political system of State B. Subsequently, in Chapter 3 the legal framework for cyber influence operations was set out and analysed, focusing on intervention and other (non-coercive) forms of interference constituting violations of sovereignty.

This chapter describes and assesses three actual influence operations thereby focusing on those aspects which were conducted in, but mainly through, cyberspace. The description of the cases is based on the sequence of preparation, execution and exploitation of the operation. In each case the intent and purpose of the influence operations are highlighted, as well as the cyber-related activities and how they make use of the attributes of cyberspace to reach audiences and, consequently, how these audience are susceptible to the content in order to generate effects.

The cases used are the 2016 United Kingdom referendum on the EU, the 2016 United States presidential election, and the 2017 French presidential election. The rationale for choosing these cases instead of other influence operations lies in the State to State character of the influence operations and the availability and accessibility of data and existing research on these cases. The analysis of the cases does not intend to provide evidence on a possible attribution of the cases. This research takes the assumed involvement of the Russian Federation in these cases as a given.

The sub-question of this Chapter is: *"How were the influence activities executed during the 2016 UK EU referendum, the 2016 US presidential election, the 2017 French presidential election?"*

The chapter starts with depicting the analytic framework of influence operations as described in the key findings of Chapter 2 with generic Russian Federation influence operations as illustration (4.1). Section 4.2 and the following sections describe the three influence operations resulting in key findings in 4.5 that serve as input for the legal appreciation and synthesis in the next chapter.

Section 4.1.: The Analytic Framework of Influence Operations

"Three hostile newspapers are more to be feared than a thousand bayonets."[1]

"At the risk of stating the obvious, the era of cyber war is here"[2]

Many States are involved in cross border influence operations including North Korea,[3] Iran,[4] the Russian Federation (RF)[5] and though the activities of these States are well-documented, it does not exclude the existence of influence activities from Western States including the United Kingdom (UK)[6] and United States of America (US).[7] Moreover, influence operations are not unique in this present day and age or in cyberspace,[8] during the Cold War period psychological influence operations by the USSR (the legal predecessor of the RF) and the US were omnipresent.[9]

[1] A quote by Napoleon, thus Cardinal Newman, paraphrasing Marshall McLuhan, Understanding Media: The Extensions of Man, International Journal of McLuhan Studies, 1994, p. 13.

[2] James Long, "Stuxnet : A Digital Staff Ride," Modern War Institute, 2019, https://mwi.usma.edu/stuxnet-digital-staff-ride/.

[3] Quentin E. Hodgson, "Understanding and Countering Cyber Coercion," *International Conference on Cyber Conflict, CYCON* 2018-May (2018): 73–88. pp. 77-79. Howard and Bradshaw argue that in 2018 48 States have executed influence operations in some 70 States, see: Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation," 2019. pp. 3-4.

[4] Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, 2018. pp. 135 ff. regarding activities in Iraq and Syria.

[5] Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice," *The American Society of International Law* 112, no. 4 (2018): 583–657. pp. 655-656; Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," 2019. pp. 1-2; United States District Court, Indictment (United States v Andrienko) "Sandworm" (2020).

[6] Max Blumenthal, "Reuters, BBC, and Bellingcat Participated in Covert UK Foreign Office-Funded Programs to 'Weaken Russia,' Leaked Docs Reveal," The Gray Zone, 2021, https://thegrayzone.com/2021/02/20/reuters-bbc-uk-foreign-office-russian-media/.

[7] On recent US activities in cyberspace see i.a. Robert Chesney, "The Domestic Legal Framework for US Military Cyber Operations," *Hoover Institution Aegis Paper*, 2020. p. 4.; Herbert S. Lin, "On the Integration of Psychological Operations with Cyber Operations," *Lawfare*, 2020, 1–3.; United States Cyber Command, "Achieve and Maintain Cyberspace Superiority," 2018.

[8] 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. 46; Media Ajir and Bethany Vailliant, "Russian Information Warfare : Implications for Deterrence Theory," *Strategic Studies Quarterly*, 2018, 70–89. p. 72; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," 2018., p. 3.

[9] Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773–816. pp. 779-782; Henning Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law," *Israel Law Review* 53, no. May (2020): 189–224. pp. 193-195. See also: Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020).

The thesis takes the view of the initiating or author State (State A) of influence operations. Therefore, the activities are described from the perspective of the RF, which was allegedly the, or one of the, initiator(s).[10]

Though the cases described differ in topic,[11] effect, intensity and probable degree of RF involvement, in general terms the influence operations follow a similar pattern: a) Preparing influence operations entails defining the intent, selecting the strategic narrative, and operationalising the strategic narrative into one or several frames; b) Then, executing the influence operation via cyber-related activities: disinformation, trolling, leaking and political grooming; c) Finally, exploiting successful cyber-related activities utilising the specific attributes of cyberspace to magnify and amplify the cyber-related activities.

[10] The cases are far from unique. UK private company 'Strategic Communication Laboratory (SLC)' for instance, has been involved in over 30 election and referendum campaigns including Australia, Kenya, Brazil and France. House of Commons Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report," 2019. bullet 275, p. 78; see also Bradshaw and Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." p. 5. But more in general, both the US and the Russian Federation have a 75-year history in meddling in elections abroad; Erik Brattberg and Tim Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks," 2018. pp. 3-4.

[11] Referendums differ from elections not least since a referendum is most often related to a single topic. See: Ece O. Atikcan, Richard Nadeau, and Eric Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums* (McGill-Queen's University Press, 2020). pp. 9-10.

Influence Operations:

- Preparation
    - (political) Intent
    - Strategic Narrative
    - Framing
- Execution cyber-related activities
    - Disinformation campaign
    - Trolling campaign
    - Leaking
    - Political Grooming
- Exploitation via social media
    - Amplify and Magnify
    - Illusion of truth

Figure 4 - 1 The phases of an Influence Operations

4.1.1. Preparation

First the objective of the State is assessed as an expression of the State's intent. As mentioned in § 2.2.1, the guiding objective of the RF is to create strategic confusion in Western democratic States[12] by undermining the concept of truth[13] and, related to that, alluding to the success and strength of the autocratic form of government as supported in the RF. The intent of the State derives from its vital interests and is reflected in the State's attitude and perception of the world.

[12] Alina Polyakova et al., "The Kremlin's Trojan Horses," 2016. p. 4; Kragh and Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case." pp. 778 ff; Nathan K. Finney, *On Strategy: A Primer*, ed. Nathan K. Finney, *US Army Combined Arms Center* (Combast Studies Institute Press, 2020). p. 74; P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018). pp. 106-107; Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, D.C.: Georgetown University Press, 2020). p. 6.

[13] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," *The Interpreter*, 2014. p. 15; Michael J Mazarr et al., *Hostile Social Manipulation Present Realities and Emerging Trends*, 2019. p. 61.

Second, the intent is articulated in the diplomatic, but mainly the informational instrument of power via calibrated strategic narratives. In the RF cases as mentioned in § 2.2.2 the intent is to create strategic confusion in Western democracies and the generic narratives used relate to the anti-European Union (EU), anti-NATO and/or the anti-liberal democracy narratives.[14]

Third, the narrative must be operationalised by scripting a frame or frames,[15] given the specificities, in this case related to the UK EU referendum, the US and French presidential elections. Strategic narratives do not automatically affect a targeted audience as the content or form of strategic messaging needs to be shaped to align with preferences and heuristics of a specific audience and to make the audience receptive to the narrative. Framing aims to create a script which will incline the audiences of State B to make predetermined decisions, or induce a conditioned reflex based on their heuristics, in a way preferable to State A, which is executing the assertive influence operation. Therefore, framing will need to triangulate a) a strategic narrative, b) divisive topics within a society that will produce an effect by making use of the communication dynamics in the public sphere of a society, and c) audiences' preferences and heuristics, revolving around an event, such as an election, a referendum or a pandemic such as Covid-19.[16] Scripting and framing efforts can make use of differences between societal groups, accentuate minority groups' feelings of rejection and neglect, fuel internal divisions over political issues or exploit tensions between neighbouring countries. The frames designed do not need to be true but need to appear realistic or probable, seeming to be indigenous to the target State. Frames can make use of social heuristics *inter alia* (i.a.) using a respected politician, scholar or celebrity to anchor the frame to authority.[17] Creating frames requires data on the demography of the audience and metrics on the audiences' biases before targeting specific audiences with divisive content. The more refined the data, the more effective the influence operation. During this phase of the influence operation,

[14] Rachel Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom," *CSIS*, 2020. pp. 7-10, thereby making use of the difference within these alliances of countries taking a hard-line on Russia and those preferring the path of dialogue. See § 2.2.2 and Laura Rosenberger, "Making Cyberspace Safe for Democracy," *Foreign Affairs* 99, no. 3 (2020): 146–60.; Jean Baptiste Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem" (Council, Atlantic, 2019). p. 44; 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. 642.

[15] George Lakoff, "Framing the Dems: How Conservatives Control Political Debate and How Progressives Can Take It Back," *The American Prospect*, 2003. p. 32; George Lakoff, *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics* (Penguin, 2009). pp. 22 ff. See also § 2.2.4. under 'framing'.

[16] It has been suggested that in the US Afro-American people are more prone to suffer from Covid-19 than persons of other ethnicities. The causality is however not necessarily related to ethnicity but social and environmental factors including health. See: Robert Booth and Caelainn Barr, "Black People Four Times More Likely to Die from Covid519 , ONS Finds," The Guardian, 2020, https://www.theguardian.com/world/2020/may/07/black-people-four-times-more-likely-to-die-from-covid-19-ons-finds.; Kia Lilly Caldweel and Edna Maria de Araújo, "COVID-19 Is Deadlier for Black Brazilians, a Legacy of Structural Racism That Dates Back to Slavery," The Conversation, 2020, https://theconversation.com/covid-19-is-deadlier-for- black-brazilians-a-legacy-of-.; Tiffany Ford, Sarah Reber, and Richard V. Reeves, "Race Gaps in COVID-19 Deaths Are Even Bigger than They Appear," Brookings Institute, 2020, https://www.brookings.edu/blog/up-front/2020/06/16/race-gaps-in-covid-19-deaths-are-even-bigger-than-they-appear/.

[17] Robert B Cialdini, *Influence: The Psychology of Persuasion*, Rev. ed. (New York SE - xiv, 320 pages : illustrations ; 24 cm: Harper, 2007). pp. 208 ff. Cialdini argues that authority is related to title, status or clothing of persons referring to the 1965 Milgram study on obedience.

data are crucial to pinpoint the socially divisive topics and heuristics of specific groups. The data can be extracted via manipulative harvesting by data-mining firms such as Cambridge Analytica, or via a hack. Hard-cyber activities could, therefore, support a soft-cyber operation during the preparation phase.

4.1.2. Execution

A frame creates templates in which all further activities, content and communications can be embedded. The next step is the execution of the influence operations in which State A engages the targeted audiences of State B. During the execution phase, the framed narratives target the audiences via cyber-related activities, ranging from the leaking of non-public information, disinformation-, trolling-, and political grooming campaigns. These activities, such as disinformation campaigns, are not unique to cyberspace and can also be executed in physical domains.[18] However, cyber-related activities of influence operations are soft-cyber operations, or social media operations which use cyberspace as a vector to transmit manipulated or disclosed content. During these activities the frames made are injected into the opponent's society, utilising the virtual dimension of cyberspace as a vector for relaying content.

4.1.3. Exploitation

Finally, cyber-related activities such as disinformation campaigns which are successful need to be exploited. Social media are used to increase reach and repetitive effect of the content. Magnifying and amplifying will validate content that fits the form and language of the dynamics of society and is aligned with the preferences and biases of the audience. The possibility to repeat messages via bots or human agents is unique to cyberspace. The exploitation phase, therefore, contributes to addressing subconscious heuristics and can create the illusion of truth, the acme of susceptibility.

[18] During the Cold War period influence operations were ideologically inspired, leading to the creation of broadcasting institutions such as Radio Free Europe, or the US funding of anti- communist magazine such as Der Monat, Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*. pp. 19-23; Or the Russian frame that Aids was developed in US laboratories (Operation Infektion) Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*.; Elswah and Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)." p. 641.

Section 4.2.: The 2016 UK EU referendum

Should the United Kingdom remain a member of the European Union or leave the European Union?[19]

We have seen nothing that persuades us that Russian interference has had a material impact on the way in which people choose to vote in elections. It is not that they have not tried, but we have not seen evidence of that material impact.[20]

4.2.1. The path to the EU referendum

On 23 June 2016 51.9% of the voters in the UK voted to leave the EU in the consultative 'United Kingdom European Union membership referendum'.[21] On 29 March 2017 the UK government notified the EU that it invoked Article 50 of the Treaty of the EU.[22] The withdrawal process was due on 29 March 2019, but was extended several times.[23] On 31 January 2020 at midnight, the withdrawal agreement came into force.

The origin of the referendum lies in the so-called Bloomberg speech by UK Prime Minister (PM) David Cameron on 23 January 2013,[24] in which he mentioned that a referendum on the UK membership of the EU was to be held if a Conservative government would be re-elected. Cameron's proposal for a referendum was a concession to the Eurosceptics within his Conservative party, and an expression of the general dismay with the EU-UK relationship. Though the Conservatives were the largest party after the 2015 general election, they did not gain a majority in the House of Commons and the Parliament was hung. The reason for this

[19] The question of the 23 June 2016 referendum, see: Elise Uberoi, "European Union Referendum 2016 Briefing Paper," House of Commons Library, no. CBP 7639 (2016): 1–40.

[20] Quote by the Rt Hon Jeremy Wright during the 24 October 2018. Evidence session. Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report." bullet 241, p. 70.

[21] The difference between Leave and Remain was 1.269.501. Given the bipartisan system (zero-sum) this difference was caused by 631.800 votes which is 1,37% of the registered voters. The overall turnout was 72,2% which is higher than previous general elections (66,2% in 2015). See: Uberoi, "European Union Referendum 2016 Briefing Paper." p. 24.

[22] Article 50 – Treaty on European Union (TEU) 1. Any Member State may decide to withdraw from the Union in accordance with its own constitutional requirements. (2..) 3. The Treaties shall cease to apply to the State in question from the date of entry into force of the withdrawal agreement or, failing that, two years after the notification referred to in paragraph 2, unless the European Council, in agreement with the Member State concerned, unanimously decides to extend this period. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M050&from=EN

[23] The withdrawal agreement entered into force as of 1 February 2020 and the subsequent trade and cooperation agreement as of 1 January 2021. See: The European Commission, "Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01)" (2019). The European Commission, "Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part" (2020).

[24] David Cameron, "EU Speech at Bloomberg," 2013.

is the turn of the UK population towards, on the one hand, the pro-EU Liberal-Democrats and, on the other, the anti-EU UK Independence Party (UKIP).[25] Furthermore, the Scottish National Party gained many votes articulating the Scottish discomfort with the incumbent government.

In May 2015 the referendum was mentioned in the Queen's Speech, and on 17 December 2015 the EU Referendum Act, stating that the referendum was to be held before the end of 2017, received the Queen's assent. The referendum followed the electoral process of Parliamentary elections in the sense that the ballot would be cast in the 382 constituencies.[26] However, the referendum was based on national proportional representation (direct voting) and not on the traditional British voting system, for Parliamentary elections (first past the post).[27]

Since the referendum was an in-or-out choice, and due to the fact that pro-Brexit and pro-Remain sentiments were rife in all UK political parties, the referendum did not follow party affiliations. Numerous entities emerged articulating specific schools of thought or interests, but the most prominent pro-Brexit entities were 'Leave.EU', which was affiliated to UKIP politician Nigel Farage, financier Arron Banks and the data-modelling firm SCL/Cambridge Analytica,[28] and 'Vote Leave' to which Dominic Cummings, and at a later stage, software developer Aggregate IQ were attached.[29] On 13 April 2016 the UK Electoral Commission proclaimed that 'Vote Leave' and the pro-EU 'The In Campaign' (also known as 'Britain Stronger in Europe') would be the designated campaign organisations.[30]
As of 27 May, the official 'purdah' or electoral silence would commence and last until Polling Day on 23 June 2016.

The results of the referendum showed marginal differences between the Leave and Remain camps nationwide but indicated significant deviations when contemplated from the perspective of geographic, demographic or socio-economic divisions. London, Scotland and

[25] Thiemo Fetzer, "Did Austerity Cause Brexit?," *American Economic Review* 109, no. 11 (2019): 3849–86. p. 3854.

[26] 380 counties in Great-Britain, 1 for Northern Ireland and 1 for Gibraltar, see: Uberoi, "European Union Referendum 2016 Briefing Paper." p. 4.

[27] 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. 605-607.

[28] The degree to which Cambridge Analytica worked with Leave.EU is contested, see e.g.: 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). pp. 200-201.

[29] Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns," 2018. pp. 33-39; The Conservative and Labour party were both split over the issue. Their respective pro-Brexit campaigns were 'Labour Leave' and 'Conservatives for Britain'.

[30] Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. pp. 20-21; The Electoral Commission, "Electoral Commission Designates 'Vote Leave Ltd' and 'The In Campaign Ltd' as Lead Campaigners at EU Referendum," *Press Releases*, 2016.

Northern Ireland largely voted to remain, as did graduated voters,[31] voters between 18 and 29 years of age, and the middle-class voters.[32]

After the referendum several reports were published indicating irregularities during the campaigns, including criminal offences for overspending by Vote Leave,[33] and Facebook's illegal harvesting of personal data.[34] A House of Commons report even concluded that the Russian Federation had applied 'unconventional warfare' against UK voters.[35]

The 2019 final House of Commons report on disinformation and 'fake news' mentioned that 261 articles with a clear anti-EU bias had been published by RT and Sputnik, news outlets affiliated to the RF.[36] The articles, shared and forwarded via social media, could have reached 134 million 'potential impressions', twice as many as Vote Leave and Leave.EU together. Facebook later removed 289 pages and 75 accounts with a total of 790,000 followers that were linked to Sputnik.

Russian influence was already noticeable during the 2014 Scottish referendum,[37] but also after the EU referendum in the UK, malign influence campaigns tried to undermine governmental policies and agencies during the 2017 Parliamentary elections and the 2018 Salisbury Skripal poisoning.[38]

4.2.2. The objective and strategic narrative

Assuming that the RF was involved in conducting activities aimed at influencing the vote during the UK EU referendum, the alleged effect it wanted to achieve by specifically supporting the Leave-camp was 'undermining public confidence and (...) destabilising

[31] Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." p. 601.

[32] Uberoi, "European Union Referendum 2016 Briefing Paper." pp. 21-22.

[33] The Electoral Commission, "Report Concerning Campaign Funding and Spending for the 2016 Referendum on the UK's Membership of the EU," no. July (2018): 1–38.

[34] Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns." p. 2 regarding the notice of intent. See also the monetary notice of Oct 2018 Information Commissioner's Office, "Monetary Penalty Notice" (2018).

[35] House of Commons Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report," 2018. Bullet 162, p. 43; Ewan McGaughey, "Could Brexit Be Void," *Ssrn*, no. July (2018): 1–11. pp. 1-5.

[36] Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report."bullets 240-248, pp. 69-71; Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." Bullets 160-163; 168-175, pp. 43-46.

[37] Intelligence and Security Committee of Parliament, *Russia*, 2020. p. 13; Ben Nimmo, "#Election Watch: Scottish Vote, Pro-Kremlin Trolls," *DFRLab*, December 2017.

[38] Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report." Bullet 240, 69; United States District Court, Indictment (United States v Andrienko) "Sandworm," 20–316. pp. 39-41.

democratic states',[39] to weaken the UK internally and diminish its position in the world,[40] and strengthen the precarious economic position of Russia.[41] Weakening the UK would inadvertently also weaken EU cohesion,[42] which might subsequently change the EU position on or even enhance, lifting the sanctions against RF.[43]

The RF mobilised numerous instruments of power against the UK separately or – ironically – in coalition with the EU, to protect and further its goals and interests. The vote to leave the EU would place the value of the British pound sterling under pressure, could force PM Cameron to resign,[44] causing further political disruption. Moreover, it would be a retaliation for sanctions against Russia imposed after its annexation of the Crimea. The list of sanctions and restrictive measures – back and forth - is substantial[45] and includes restriction on energy related items,[46] the freezing of assets,[47] barring EU officials from entering the country, and non-issuance of visa to residents of Crimea. These measures are related to the 2014 Crimea crisis, the 2014 Paris Climate Agreement,[48] the 2014 MH 17 downing and the 2015 Russian presence in Ukraine, but also reflect the UK's 'innate resilience'[49] towards Russia.[50]

Though the Russian military intelligence service GRU[51] has been affiliated with numerous hard-cyber hacking operations to gain access and infiltrate networks such as TV5 Monde,[52] and later the Democratic National Committee (DNC) (see § 4.3), World Anti-Doping Agency

[39] Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." bullet 160.

[40] Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom." pp. 4-5.

[41] McGaughey, "Could Brexit Be Void." p. 5; Intelligence and Security Committee of Parliament, *Russia*. pp. 1-2.

[42] Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom." p. 8.

[43] Steve Rosenberg, "EU Referendum: What Does Russia Gain from Brexit?," no. June (2016).

[44] Rosenberg.; McGaughey, "Could Brexit Be Void." pp. 5-6.

[45] See e.g.: Council of the European Union, "Council Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine," Official Journal of the European Union § (2014).; President of Russia, "Executive Order on Extending Special Economic Measures to Ensure Russia's of Russia Security" (2017). Related to Executive Orders No. 320 of June 24, 2015 and No. 305 of June 29, 2016. For an overview see also: Ivan Gutterman and Wojtek Grojec, "A Timeline Of All Russia-Related Sanctions," RadioFreeEuropeRadioLiberty, 2018, https://www.rferl.org/a/russia-sanctions-timeline/29477179.html.

[46] United Kingdom Department for Business Innovation & Skills, "EU Sanctions against Russia - Further Information," no. December (2014): 13.

[47] General Secretariat of the Council, "Conclusions of the European Council/ EURO 7/1/14 (20-21 March 2014)," 2014.

[48] Ewan McGaughey, "The Extent of Russian-Backed Fraud Means the Referendum Is Invalid," LSE Blogs, 2018, https://blogs.lse.ac.uk/brexit/2018/11/14/the-extent-of-russian-backed-fraud-means-the-referendum-is-invalid/.

[49] US Senate, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security" A minority staff report Committee on Foreign Relations 152nd Session, January 10, 2018, p. 116.

[50] Richard Sakwa, "Russo-British Relations in the Age of Brexit," 2018. pp. 11-15.

[51] In Russian this is the *Glavnoje Razvedyvatel'noje Upravlenije*, the ГРУ or "Main Intelligence Directorate" which is part of the General Staff of the Ministry of Defence. The main cyber-related units resorting under the GRU are APT 28 (Fancy Bear), and APT Sandworm.

[52] Gordon Corera, "How France's TV5 Was Almost Destroyed by Russian Hackers," BBC News, 2016, https://www.bbc.com/news/technology-37590375. The TV5 hacks was executed in April 2015, allegedly by APT 28.

(WADA)[53] and OPCW,[54] there is no public evidence in the EU Referendum Case that cyber infrastructure (hardware) was successfully tampered with.[55] Nor was it documented that hacks have taken place with the intent to steal, manipulate, copy or otherwise gain access to data which were in the possession of UK government or public entities, by Russia or any other (domestic) entity.[56]

Apart from using supportive economic and financial instruments,[57] the RF's main effort lay in the realm of the informational instrument of power, mainly exploiting an anti-EU narrative.[58] For quite some time the RF has intended 'to undermine European integration and the EU, in addition to its aims to sow confusion and undermine confidence in democratic processes themselves, making Brexit a potentially appealing target.'[59] This 'normative war'[60] between the RF and the EU has gradually built up and is based on a disparity in views on legitimacy and political conduct, which is reflected in domestic and international State behaviour and has a long historical standing.[61] The RF has consistently emphasised what it still considers illegal attacks on Serbia during the Kosovo crisis in 1999, the illegal attack on Iraq in 2003, the allegedly undermining influence of the EU Eastern Partnership programme,[62] the admittance of Eastern European and Baltic States to the EU, and the eastward expansion of NATO to include countries close to the Russian border. In contrast, the UK and other Western

[53] DFRLab, "# PutinAtWar : WADA Hack Shows Kremlin Full-Spectrum Approach," Atlantic Council, 2018, https://medium.com/dfrlab/putinatwar-wada-hack-shows-kremlin-full-spectrum-approach-21dd495f2e91.; Andy Greenberg, "Russian Hackers Get Bolder in Anti-Doping Agency Attack," *Wired*, 2020. The WADA hacks, likely by APT 28, started around September 2016 and will still on-going in 2019.

[54] The Organisation for the Prohibition of Chemical Weapons (OPCW). NCSC, "Reckless campaign of cyber attacks by Russian military intelligence service exposed", on *NCSC.GOV.UK*, 3 Oct 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed. The hack took place in April 2018 and was attributed to a the GRU, in cooperation with the FSB APT 29 (Cozy Bear).

[55] Though the website 'Register to vote' crashed on 7 June 2016, which could be caused by a surge of public requests, but could also allude to a foreign DDoS attack. Also, on 23 June 2016, the day of the referendum the UK power supply was targeted by hackers. See: the Summary of Public Administration and Constitutional Affairs Committee House of Commons, "Lessons Learned from the EU Referendum," 2017.; Laura Galante and Ee Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *Atlantic Council* September (2018). pp. 8-9; Rachel Ellehuus and Donatienne Ruy, "Did Russia Influence Brexit ?," *Center for Strategic and International Studies*, 2020, 1–2.

[56] Intelligence and Security Committee of Parliament, *Russia*. pp. 12-14; Ciaran Martin, "Cyber Security : Fixing the Present so We Can Worry about the Future," 2017.; David D. Kirkpatrick, "British Cybersecurity Chief Warns of Russian Hacking," The New York Times, 2017, https://www.nytimes.com/2017/11/14/world/europe/britain-russia-cybersecurity-hacking.html.

[57] Russia has deliberately mobilised instruments of power to undermine UK interests related to the campaign finance laws and the broadcasting law, e.g. UK Legislation, Political Parties, Election and Referendum act 2000, c. 41, Part IV, Chapter, Permissible donation, Section 54. https://www.legislation.gov.uk/ukpga/2000/41/section/54; UK Legislation, Representation of the People Act 1983, c. 2, Part II, Publicity at Parliamentary Elections, Section 92. http://www.legislation.gov.uk/ukpga/1983/2/section/92

[58] Rosenberg, "EU Referendum: What Does Russia Gain from Brexit?"; Intelligence and Security Committee of Parliament, *Russia*. pp. 1-2.

[59] US Senate, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security" A minority staff report Committee on Foreign Relations 152nd Session, January 10, 2018,, p. 116.

[60] Kadri Liik, "Winning the Normative War with Russia," 2018. p. 2.

[61] Polyakova et al., "The Kremlin's Trojan Horses." p. 18.

[62] Igor Gretskiy, Evgeny Treshchenkov, and Konstantin Golubev, "Russia's Perceptions and Misperceptions of the EU Eastern Partnership," *Communist and Post-Communist Studies* 47, no. 3–4 (2014): 375–83. p. 377.

democracies' narrative, after the Cold War-era, highlights the superiority of democracy and the liberal international order, labelling Russia as corrupt, suppressive and legally unreliable,[63] hence the nemesis of the Human Rights code and Environmental Agreements. The RF counters this narrative by claiming that it has fallen victim to hypocritical and corrupt Western politicians,[64] that human rights are violated everywhere and all elections are falsified.[65] These sentiments are in line with the ideology of the new type of Russian State based on 'popular trust in the leader rather than competitive elections that is superior to Western-style democracy'.[66]

4.2.3. Framing the narrative

The UK referendum provided an opportunity to employ the existing narrative against the EU. The frames construed by the UK actors, such as UKIP, BNP (the far-right British National Party), 'Vote Leave', 'Leave.EU' or 'BeLeave',[67] coalesced with the existing Russian anti-EU narrative.[68] Russian activities during the UK referendum on the EU focussed on existing differences. The cyber-related activities (e.g. disinformation campaign) 'amplified negative news about immigrants and refugees'[69] and enhanced anti-EU separatist sentiments.[70] Ellehuus argues that while "many of the factors that led to Brexit—an exaggerated fear of migration, disenfranchisement of the working classes, the urban/rural divide, and sensationalist media—were already present, Russia was quick to grasp the opportunity to exploit these grievances and associated vulnerabilities to its advantage."[71] RF tactics were such that they did not advocate a specific position, but they amplified existing anti-EU narratives by flooding the public sphere with a combination of accurate, half-true and false

[63] Liik, "Winning the Normative War with Russia." The UK fears focus on hacking, propaganda, financing and business ties, p. 45.

[64] DFRLab, "# PutinAtWar : WADA Hack Shows Kremlin Full-Spectrum Approach."

[65] Mikhail Zygar, "Why Putin Prefers Trump," Politico, 2016, https://www.politico.com/magazine/story/2016/07/donald-trump-vladimir-putin-2016-214110.

[66] Goble, P., Surkov reflects Putin Elite's hatred and fear of the people, in Windows of Eurasia, 12 February 2019. The article paraphrases Russian commentator who argues that Surkov's recent essay on the new Russian State that the ruling elite hates, distrusts, and fears the people and wants to destroy its political standing and minimize the risks it presents. This by depriving the people of legal institutions and (democratic) possibilities to influence the situation in the country.

[67] The Electoral Commission, "Report Concerning Campaign Funding and Spending for the 2016 Referendum on the UK's Membership of the EU." p. 1; Polyakova et al., "The Kremlin's Trojan Horses." pp. 20-21. Leave.EU was linked to Elizabeth Bilney and by Arron Banks (also founder of 'Better For The Country') and affiliated with UKIP's Nigel Farage. Vote Leave was founded by i.a. Dominic Cummings and was the cross party official campaign in favour of leaving the EU, affiliated with Labour Leave, Business for Britain, and Conservatives for Britain including prominent Brexiteer Boris Johnson. BeLeave was founded by Darren Grimes and focused on young Brexiteers, BeLeave was affiliated with Vote Leave.

[68] Lakoff, *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics*. p. 22.

[69] Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom." p. 5.

[70] Miguel Carreras, Yasemin Irepoglu Carreras, and Shaun Bowler, "Long-Term Economic Distress, Cultural Backlash, and Support for Brexit," *Comparative Political Studies* 52, no. 9 (2019): 1396–1424. p. 1415.

[71] Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom." p. 8.

information.[72] It stands to reason that RF based its activities on existing domestic frames,[73] rather than creating an independent frame.[74]

For the Leave-camp the EU referendum was the trigger to commence framing activities. The frames used - including 'Independence Day' (being the day of the referendum) or 'take back control'[75] - are powerful and appeal to feelings of Euroscepticism[76] and the perception that the EU and not the UK has control over the country. The frames invoke the persistent national tradition of scapegoating the EU.[77]

Taking the EU referendum as the central occurrence, the frames triangulate socially divisive topics, ingrained preferences of groups, and the anti-EU conviction around that occurrence. The socially divisive topics relate to actual political issues including migration, declining healthcare and the economic recession. Socially divisive topics urge groups in society to communicate and express views. The heuristics used invoke the confirmation, conformity or anchoring biases of groups within UK society related to anti-establishment (upper-class) issues, the lack of control due to the influx of migrants, the perceived threat from immigration, British identity, and long-term resentment against the EU.[78] The frames that were created used simplifications of topics, anchored random societal issues to the EU, made use of stereotype false suggestions aimed at blaming the EU for UK mishaps.[79] In short, the decline of the UK economy and healthcare system started in the late 1970s at the same time the UK joined the EU. Hence, the UK needed to 'take back control', suggesting that leaving the EU would invigorate the economy, the national health service and solve immigration issues.

Coupling the EU referendum to existing socially divisive topics and groups' heuristics requires the collection of data on these topics in society, but also on the demography of the

[72] Ellehuus. p. 11.

[73] Galante, L., & Ee, S., Defining Russian Election Inference, *Atlantic Council Issue Brief*, Sept 2018, p. 5.

[74] Alexey Kovalev, "Here's What Russians Think: Brexit Is Your Creature - Don't Blame It on Us (Opinion)," The Guardian, 2017, https://www.theguardian.com/books/2015/jul/17/postcapitalism-end-of-capitalism-begun.

[75] Dominic Cummings, "How the Brexit Referendum Was Won," *The Spectator*, 2017.

[76] Steve Corbett, "The Social Consequences of Brexit for the UK and Europe: Euroscepticism, Populism, Nationalism, and Societal Division," *International Journal of Social Quality* 6, no. 1 (2017): 11–31. pp. 13-14.

[77] Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. pp. 50-52 & 73-75 and Chapter 4. The Remain camp mainly used the economic loss when leaving the EU as a central theme. Remain politicians were in a lagging position as political elites and media have been blaming the EU in the last decades, so a pro-EU voice lacked credibility and appeared inauthentic.

[78] James Ball, *Post-Truth: How Bullshit Conquered the World*, *Biteback Publishing* (London, 2017). p. 60; Alex I. Macdougall, Allard R. Feddes, and Bertjan Doosje, "'They've Put Nothing in the Pot!': Brexit and the Key Psychological Motivations Behind Voting 'Remain' and 'Leave,'" *Political Psychology* 41, no. 5 (2020): 979–95. pp. 981-982.

[79] E.g. 'we want our country back', 'vote leave, take control', 'let's give the NHS the £350 million the EU takes every week', 'Turkey (76 million population) is joining the EU'. See also: Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. pp. 67-70.

population and the preferences of groups within a population.[80] In the run-up to the EU referendum personal data of potentially 1 million voters were harvested via intermediate agencies, such as AIQ supporting Vote Leave, and Cambridge Analytica, which worked for the Leave.EU.[81] These data were acquired, not via illegal cyber intrusion but by utilising the natural inclination of people to take detailed personality tests via their Facebook accounts. The data were later used to micro-target specific groups in society with bespoke messages and political adverts compatible with their opinions and beliefs. [82] Based on the data found powerful frames were generated, mainly created by the Leave camp,[83] captivating the audience or specific groups in that audience.

Russian endeavours can be seen as supporting on-going domestic operations, highlighting existing fears or division within society. The messages sought to incite fears about Muslims and immigrants and exacerbate anti-EU sentiments to help drive the vote.[84]

4.2.4. Cyber-related activities

During the UK EU Referendum the most prominent cyber-related activities of the influence operations were disinformation activities to spin reality and pushing the anti-EU narrative. The influence operation also consisted of a political grooming campaign to specifically support the 'Leave'-camps, and trolling activities to discredit democratic institutions. The trolling campaign had the aim to intensify socially divisive topics and manipulate the perception and behaviour of the British population.

The disinformation campaign was mainly a domestic campaign by political actors articulating the opinion of a large segment of the population wishing to leave the EU i.e. UKIP, Vote Leave, BNP and BeLeave.[85] As the Leave-campaign coalesced with the existing Russian anti-EU narrative, the RF used the UK EU referendum to support or discredit politicians or parties by political grooming and trolling, and seized the opportunity to sow discord by alluding to the failure of democratic systems in order to undermine the stability of Western

[80] 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. 147-149.

[81] Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report." pp. 26 ff.; Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns." A Facebook app was developed by Dr Aleksandr Kogan which harvested data of 87 million voters including 1 million in the UK, p. 8.

[82] Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns." p. 9.

[83] Cummings, "How the Brexit Referendum Was Won."

[84] David D. Kirkpatrick, "Signs of Russian Meddling in Brexit Referendum," The New York Times, 2017, https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html.

[85] Pawel Dlotko and Simon Rudkin, "An Economic Topology of the Brexit Vote," *Arxiv*, 2019, 1–43. pp. 1-4 & 41; Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." pp. 69-72; Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." p. 642.

democracies,[86] thereby magnifying anti-Muslim feelings, exaggerating the immigration issue and highlighting the economic and financial problems of the country,[87] which reflect internal predicaments and are not inherently related to EU membership.

The disinformation campaign of the Leave camp revolved around three main EU-related issues which caused degrees of social division: immigration, trade (economy) and UK contributions to the EU.[88] During the disinformation campaign, the high levels of immigration and the costs of EU membership were framed as reasons for the declining service levels of the National Health Service (NHS).[89] An aspect of the disinformation campaign within the frame of 'taking back control' was the notion that the EU cost the UK £350 M per week, while this huge amount of money could also be spent on the NHS. Related topics which were intensified by existing resentments, such as fiscal cuts, unemployment, and a lack of proper housing, all of which were not directly related to the EU.

The Russian involvement in the disinformation campaign itself, where related is concerned, is marginal. However, it was reported that between 1 January 2016 and the referendum on 23 June, the RF controlled internet outlets, RT[90] and Sputnik, published 261 articles related to Brexit which contained fabricated or distorted content with an anti-EU sentiment.[91] All articles were negative (anti-EU) in content, though some were broadly factual.[92] An example of this is the headline used in a Sputnik article: 'Bank of England in Brexit: no need to panic, yet'. The headline was fabricated and did not reflect the interview referring to in the article.[93] Between 1 and 8 February 2016 alone, Sputnik ran 14 stories on 'Brexit' related issues with a strong bias toward the Leave-camp.[94]

[86] Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom." pp. 10 & 27; Kovalev, "Here's What Russians Think: Brexit Is Your Creature - Don't Blame It on Us (Opinion)."

[87] Fetzer, "Did Austerity Cause Brexit?" pp. 3882 ff; Cummings, "How the Brexit Referendum Was Won." See the three forces that changed the opinion on the EU (immigration, 2008 financial crisis, Euro-crisis); Macdougall, Feddes, and Doosje, "'They've Put Nothing in the Pot!': Brexit and the Key Psychological Motivations Behind Voting 'Remain' and 'Leave.'" p. 979.

[88] Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." pp. 613-615.

[89] Fetzer, "Did Austerity Cause Brexit?" p. 3855; Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." pp. 616-617; Cummings, "How the Brexit Referendum Was Won."

[90] Formerly known as 'Russia Today'.

[91] Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." Para 162; 89 up, "Putin's Brexit? The Influence of Kremlin Media & Bots during the 2016 UK EU Referendum," 2018. Slide 8; Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 9.

[92] The House of Commons final report, underlined by the US Senate minority report, concludes that Kremlin-aligned media published a lot of unique articles about UK referendum, especially anti-EU posts were popular, making use of Twitter, Facebook, Instagram, and You to fuel social divisions. See: Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report." pp. 69-71; 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. 116 ff.

[93] Sputnik News, "Bank of England on Brexit : No Need to Panic, Yet," Sputnik, 2016, https://sputniknews.com/europe/201602051034290031-business-investments-brexit-europe/.

[94] Nimmo argues that 'coming from outlets (i.e. Sputnik) paid for by the Russian government, it looks distinctly like an attempt to influence the UK debate'. See: Ben Nimmo, "Putin's Media Are Pushing Britain For The Brexit," The Interpreter, 2016, https://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/.

The foreign campaigning support (political grooming) from the RF was intense during the EU referendum,[95] though only partially executed via cyberspace. The RF was suspected of funding national campaigns, Leave-affiliated politicians and parties,[96] and broadcasts and conveying political messages.[97] Russian news outlets, including RT and Sputnik, were active in supporting the leader of the UK Independence Party, Nigel Farage, by broadcasting or amplifying his statements[98] while he was attacking then-PM Cameron during the so-called '#Piggate'-affair.[99]

The trolling activities supported the political grooming. They could spread mal-information harassments, inflammatory[100] and discriminatory comments using Facebook accounts, blogs, user groups, Twitter, and media outlets such as Sputnik and RT.[101] Their content sought to widen the division between the Leave and Remain camp, thus seeking to undermine the common values of the UK population, and weakening the public discourse.[102] The trolling campaign targeted EU politicians while at the same time supporting UK politicians favouring a Brexit, in particular UKIP leader Farage and Conservative politician Boris Johnson.[103]

4.2.5. Exploiting social media

Though the RF merely facilitated and supported the ongoing domestic cyber-related activities, it had a more dominant role in exploiting social media to amplify and repeat the existing disinformation campaigns of the Leave-camp to support their own political leaders or slander the opposite camp.

[95] Ellehuus, "Mind the Gaps: Assessing Russian Influence in the United Kingdom." p. 9.

[96] 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. 116 ff.

[97] Although foreign campaign funding is not permitted, the law does allow donations by companies carrying business in the UK, including from non-British corporations registered in the EU. The National Crime Agency is investigating the 8.4 M pound donations of Mr Arron Banks to the Leave campaign, a donation derived from gold and diamond acquisition involving the Russian Ambassador to the UK, Mr Alexander Yakovenko. See also: House of Commons: Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Interim Report, 2018 bullets 177, 185-187; There was not only a link to Russia. The Democratic Unionist Party allegedly receive a 435K pound donation by Saudi-Arabia. See: McGaughey, Ewan, Could Brexit be void? SSRN publications, 2018, p. 5.

[98] Nimmo, "Putin's Media Are Pushing Britain For The Brexit."

[99] Jean Baptiste Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies," *CAPS of the Ministry for Europe and Foreign Affairs and IRSEM of the Ministry for the Armed Forces*, 2018. p. 77; Abby Tomlinson, "The Most Shocking Thing about #Piggate Is That It Wouldn't Be the Worst Thing David Cameron Has Done," *Independent*, September 22, 2015. The 'Piggate -affair' refers to an anecdote, published in an unauthorised biography of David Cameron, in which Cameron performed indecent acts on a pig as part of an initiation ritual during his university years.

[100] 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." p. 116.

[101] Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." Para 162-163, pp. 43-44.

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

[103] RT news, "'Part-Kenyan' Obama Dislikes Britain for Its Colonial Past , Say 'Dog Whistle Racist' Boris & Farage," RT, 2016, https://www.rt.com/uk/340648-obama-johnson-farage-kenya/.; Sputnik News, "Tusk 's EU Reform Proposals ' Hardly Worth Waiting for ' - UKIP Leader," Sputnik, 2016.

To generate momentum to the suggested linkages created in the frames, the exploitation of social media is pivotal. The message, as an expression of the narrative can be supported by a number of strands. Amplifying and repeating the domestic messages by RF agents may enhance social discord,[104] or cause general confusion and invoke emotional responses to the ruling government. Exploiting messages via social media could also pro-actively target potential counter-narratives or undermine the credibility of persons, groups or entire nations.

Media outlets amplify the frames and the subsequent cyber-related activities. Russia mobilised 419 so-called 'false front' Twitter accounts,[105] ran by the St Petersburg IRA, to circulate language highlighting the social discord with a focus on anti-Muslim texts. Russia also made use of Twitter bots that echoed or retweeted messages with a 'Leave-related' context.[106] This sentiment amplification in the months preceding the EU referendum was exacerbated by bloggers disseminating anti-Western messages,[107] thus contributing to misleading stories and deceitful stereotyping. Russia also sought to affiliate authoritative actors to magnify the messages, for example key members of the BNP, but first and foremost UKIP's Nigel Farage.[108] To the average (UK) citizen, it is difficult to make the distinction between a 'human' account and a bot, but even more between a UK and a Russian-based operator. Hence the registered voters will be deceived and cannot freely make up their minds.

Narayanan et al. argue that 'junk news websites and political bots are crucial tools in digital propaganda attacks – they aim to influence conversations, demobilize opposition and generate false support'.[109] But at the same time, they conclude that the reach of the Russian activities was marginal since the (then) 2,752 IRA Twitter accounts hardly mentioned Brexit and Russian (junk) news originating from RT or Sputnik news topics was not widely shared.[110] A research by Gorodnichenko et al. showed that there was a peek in Tweets on the day of the referendum (23 June 2016) and on the day after when the results were made public. In

[104] Adam, K., & Booth, W., 'Rising Alarm in Britain over Russian Meddling in Brexit Vote', in *The Washington Post*, 17 Nov 2017. https://www.washingtonpost.com/world/europe/rising-alarm-in-britain-over-russian-meddling-in-brexit-vote/2017/11/17/2e987a30-cb34-11e7-b506-8a10ed11ecf5_story.html?noredirect=on&utm_term=.6e2d163c5c87

[105] Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 9; Robert Booth et al., "Russia Used Hundreds of Fake Accounts to Tweet about Brexit , Data Shows," The Guardian, 2017, https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

[106] Narayanan et al., "Russian Involvement and Junk News during Brexit." 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.

[107] Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." pp. 8-9.

[108] Polyakova et al., "The Kremlin's Trojan Horses." pp. 21-22; 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." p. 117.

[109] Narayanan et al., "Russian Involvement and Junk News during Brexit." p. 2.

[110] Narayanan et al. pp. 2, 4-5.

contrast, in the weeks before the referendum there was only limited activity from these allegedly Russian accounts.[111]

Moreover, researchers at Swansea and Berkeley University – not specifically studying Russian influence - have analysed more than 2 Million tweets that were sent between 24 May and 23 July.[112] The results provide underline the so-called 'echo chambers'-effect of social media, meaning that people 'tend to select themselves into groups of like-minded people so that their beliefs are reinforced while information from outsiders might be ignored.' [113] This would mean that social media platforms like Twitter enhance ideological segmentation and make information more fragmented.

It may be concluded that the Russian influence operation magnified the existing sentiments about the on-going domestic influence operations between the Leave and Remain Camp, rather than change attitude or behaviour.

4.2.6. Generating effects

The RF influence operation did not stop on Polling Day, 23 June 2016. In the years after the Brexit, the RF has been building on the discord sowed during the Brexit campaign.[114] In discussing the social 'post-Brexit' effects, Corbett highlights that the UK EU referendum has emphasised and articulated existing or latent sentiments and frustrations.[115] The disinformation campaign by the Leave camp, supported by the persistent RF influence operation, could have a long-term effect on the attitude of the British people.[116] The influence campaign during and after the EU referendum divided the country not along traditional

[111] Gorodnichenko, Pham, and Talavera, "Social Media, Sentiment and Public Opinions: Evidence From #Brexit and #Uselection." p. 49; Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." p. 43; Reuters Staff, "Russian Twitter Accounts Promoted Brexit Ahead of EU Referendum : Times Newspaper," *Reuters*, November 15, 2017.

[112] Gorodnichenko, Pham, and Talavera, "Social Media, Sentiment and Public Opinions: Evidence From #Brexit and #Uselection." p. 46.

[113] Gorodnichenko, Pham, and Talavera. p. 3.

[114] "UK Cyber-Defence Chief Accuses Russia of Hack Attacks," *BBC News*, November 15, 2017. See also the support given to Brexiteer Rees-Mogg, Rees-Mogg followers on twitter rose from 100.000 to 230.000, most likely amplified by Russian bots. See: Isobel Cockerell, "How Russian Bots Amplify Britain's Jacob Rees- Mogg," *Codastory*, February 2019.

[115] Corbett, "The Social Consequences of Brexit for the UK and Europe: Euroscepticism, Populism, Nationalism, and Societal Division." pp. 23-27.

[116] Carreras, Irepoglu Carreras, and Bowler, "Long-Term Economic Distress, Cultural Backlash, and Support for Brexit." p. 1416.

political affiliations either to Labour or to Conservatives,[117] but instead between groups with different socio-economic and educational backgrounds.[118]

The RF has indeed executed influence operations in the UK during the EU referendum or at least elements of an influence operation in which the RF has magnified and repeated ongoing influence activities, generally in support of the Leave camp. The UK EU referendum was not the last influence operation of the RF. In November 2017, Prime Minister May - referring to the 2017 UK general elections - expressed disapproval of Russian meddling aiming to sow discord and undermine the UK democracy.[119]

The question remains what impact the RF activities have had on (the outcome of) the EU referendum? Bastos and Becker argue that the RF activities did not necessarily mean that foreign interferences sway the popular vote. They argue that the outcome of the UK EU referendum was rather the result of a 40-year effort to extricate the UK from the EU, resulting from a reluctance to fully commit itself to the EU as a supranational institution.[120]

Furthermore, the UK government and its agencies take an evasive stance on the RF influence during the UK EU referendum. The House of Commons report on disinformation and 'fake news' states that there is 'clear and proven Russian influence in foreign elections',[121] whilst the ICO in a letter to Parliament concluded that there has been no misuse of data.[122] However, the evidence remains circumstantial,[123] this not least since Facebook – harvesting personal data -,[124] Cambridge Analytica and the UK government until the House of Commons

[117] Fetzer, "Did Austerity Cause Brexit?" p. 3851. This in contrast to the situation in the US and France as described in 4.3 and 4.4.

[118] Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. p. 121, Atikcan et al. speak about the generational, educational and affluence gap; Fetzer, "Did Austerity Cause Brexit?" p. 3884; Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." pp 605-607; Marco T. Bastos and Dan Mercea, "The Brexit Botnet and User-Generated Hyperpartisan News," *Social Science Computer Review* 37, no. 1 (2019): 38–54. pp. 39-40.

[119] In this speech PM May stated: "So I have a very simple message for Russia. We know what you are doing. And you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of Western nations to the alliances that bind us. The UK will do what is necessary to protect ourselves, and work with our allies to do likewise." See: Prime Minister's Office, "PM Speech to the Lord Mayor's Banquet," 2017, https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.

[120] Bastos and Mercea, "The Brexit Botnet and User-Generated Hyperpartisan News." p. 39.; Becker, Fetzer, and Novy, "Who Voted for Brexit? A Comprehensive District-Level Analysis." p. 604; Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*. pp. 96-100.

[121] Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report." bullet 237 pp. 68; Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." pp. 71-72.

[122] Information Commissioner's Office, "ICO Investigation into Use of Personal Information and Political Influence - Letter to Julian Knight MP," 2020.; Izabella Kaminska, "ICO ' s Final Report into Cambridge Analytica Invites Regulatory Questions," Financial Times, 2020, https://ftalphaville.ft.com/2020/10/06/1602008755000/ICO-s-final-report-into-Cambridge-Analytica-invites-regulatory-questions/.

[123] The clearest influence refers to the, non-cyberspace, RF financial links with the largest donator to the Leave camp, Mr Arron Banks. The link between the donation and activities of AIQ, SCL or Cambridge Analytica is more opaque.

[124] Antonia Garraway and Tim Robinson, "Russian Interference in UK Politics and Society - House of Commons Debate Pack," no. December (2017). p. 3.

inquiry between 2017 and 2019,[125] have denied any Russian influence.[126] Moreover, in 2019, two e-petitions for inquiries were submitted. The first petition questioned the legitimacy of the EU referendum since the illegal overspending as concluded by the Electoral Commission could have affected the outcome of the vote. The second focused on misconduct due to possible interference from foreign actors and governments. The government responded to these petitions on 15 April and 24 April 2019 respectively, stating that 'there are no plans to establish a public inquiry on the conduct during the 2016 EU Referendum. The Government has not seen evidence of successful interference in UK democratic processes'.[127]

4.2.7. Concluding remarks

It can be concluded that the disinformation campaign revolving around the frame to 'take back control' - which was the main influence effort during the 2016 EU Referendum - was mainly an ongoing domestic campaign by UK actors who wished to leave the EU. The domestic parties and factions of the Leave-camp were well aware of the latent (anti-EU) sentiments, frustration and ingrained biases of segments of the British population, and able to exploit these by coupling them to socially divisive topics regarding economy, the healthcare system and migration.

Certainly, the influence operation during the UK EU referendum provided the RF with an opportunity to exploit the existing anti-EU narrative. Nonetheless, it is unlikely that the Russian Federation executed a fully-fletched influence operation. The RF did not start the influence operation in the UK but seized the momentum of the referendum since it coincided with the existing anti-EU narrative. The RF, once involved in the UK EU referendum, exploited the existing narratives and scripted frames made by the Leave-camp. In this way, it is unlikely that the British population was aware that certain activities stemmed from abroad, providing the RF with plausible deniability.[128]

RF's main activities were designed to exploit social media, amplifying and repeating content in support of the domestic disinformation campaigns of the 'Leave camp'-actors, meanwhile seizing the opportunity to sow discord and alluding to the failure of democratic systems in order to undermine the stability of Western democracies. RF activities supported an ongoing

[125] Digital Culture Media and Sport Committee, "Disinformation and 'Fake News': Final Report."

[126] "Subversion: Russia: Written Question - 113484 by Liz Saville Roberts MP," UK Parliament, 2017.

[127] UK Government and Parliament, "Halt Brexit For A Public Inquiry (Petition 241848)," UK House of Commons Library, 2019, https://petition.parliament.uk/archived/petitions/241848.; UK Government and Parliament, "To Establish A Public Inquiry Into The Conduct Of The 2016 EU Referendum (Petition 250178)," UK House of Commons Library, 2019, https://petition.parliament.uk/archived/petitions/250178.

[128] Alina Polyakova and Spencer P Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition the New Geopolitics," *Brookings - Robert Bosch Foundation*, no. March (2018). p. 4; Radley Hanlon, "It's Not Just Facebook: Countering Russia ' s Social Media Offensive," 2018. p. 2.

domestic influence operation, mainly by executing political grooming and trolling activities. The political grooming, which was only partially executed via cyberspace,[129] was specifically meant to support the 'Leave camp'. The trolling activities aimed to discredit democratic institutions or incumbent political leaders. Both cyber-related activities enhancing the profile of the Leave politicians irrelevant of their political background, seeking to increase the dichotomy between the Leave and Remain camp.

Section 4.3.: The 2016 American Presidential Election

"I do not think foreign nationals have any business in our political campaigns.
They cannot vote in our elections so why should we allow them to finance elections?
Their loyalties lie elsewhere;
They lie with their own countries and their own governments"[130]

Putin aimed for chaos,
and Donald Trump was the chaos candidate in 2016.[131]

4.3.1. The path to the US presidential election

The Russian Federation (RF) operation to influence the 2016 presidential election of the United States of America (US) were prepared well in advance. The first agents of the Internet Research Agency (IRA) began targeting audiences in the US in line with the Active Measures-doctrine as of the spring 2014,[132] with the goals 'of sowing discord in the U.S. political system."[133] By June 2014 the IRA agents also travelled to the US.[134]

[129] Digital Culture Media and Sport Committee, "Disinformation and ' Fake News ': Interim Report." pp. 50-51. Most of the activities in this realm were administered via regular though dubious financial procedures using loop-holes in legislation, hence not specifically making use of the attributes of cyberspace.

[130] Senator Bentsen during the Senate Watergate Committee, Proceedings of Congress and General Congressional Publications, "Congressional Record (Bound Edition) Volume 120," (1974).

[131] Alex Finley, John Sipher, and Asha Rangappa, "Why the 2020 Elections Will Be A Mess: It's Just Too Easy for Putin," *Just Security*, February 2020.

[132] Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," *Select Committee on Intelligence United States Senate*, (2017). p. 2; 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. pp. 4-5 & 42. For more background on the IRA, see Renee Diresta et al., "The Tactics & Tropes of the Internet Research Agency," *New Knowledge*, 2018. pp. 4-10.

[133] Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," vol. I and II, 2019. p. 14; Clint Watts, "Disinformation: A Primer in Russian Active Measures and Influence Campaign," *Statement Prepared for the US Senate Select Committee on Intelligence Hearing*, (2017). pp. 34-36.

[134] Todd C Helmus, "Social Media and Influence Operations Technologies: Implications for Great Power Competition," in *Strategic Assessment 2020*, ed. Thomas F. Lynch (National Defense University, 2020), 153–68. p. 156; United States District Court, Indictment (United States v Internet Research Agency LLC) (2018). pp. 12-13.

RF-affiliated agents have tried to corrupt the US voting infrastructure as well as to influence the US voters. Though 'Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections', no evidence was found that 'vote tallies were altered or that voter registry files were deleted or modified'.[135] Activities performed by RF agents to undermine 'confidence in U.S. democratic institutions and voting processes'[136] were the scanning of election-related infrastructure in at least 21, but probably in all 50 US states.[137] Furthermore, they accessed election infrastructure for instance in Illinois in June 2016, most likely extracting voter-registration data but refraining from deleting these data. RF agents also directed their activities at US voting systems, voting machine companies, and observed polling locations.[138]

To influence the voters the IRA used virtual persona impersonating US citizens, to operate their social media accounts and numerous group pages in order to address divisive US political and social topics. Initially the IRA agents focussed on Facebook, YouTube, and Twitter, but later on Tumblr and Instagram accounts were added.[139] The accounts were used to induce fictitious US grassroots initiatives to support - or protest against - US political and social activists related to either the Tea Party action group, Black Lives Matter, or anti-immigration platforms.[140]

As of February 2016 the IRA started to criticize Democratic candidate Hillary Clinton and to support her antagonist Sanders and (later) the Republican candidate Donald Trump instead.[141] The social media (Twitter) accounts or (Facebook) pages were meant to instigate social discord,[142] by being overly conservative ('Being Patriotic', 'Secured Borders'), seek social justice ('Black Matters', 'Blacktivist') or endorse religious and gender freedom ('United Muslims of America', 'LGBT United').[143] To illustrate this, the fabricated story on Facebook that Pope Francis endorsed Trump for President had 960,000 shares, reactions, and comments;

[135] 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. p. 5. See also: Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. p. 81.

[136] 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. 5.

[137] United States Senate Committee on Intelligence. pp. 10-21.

[138] United States Senate Committee on Intelligence. pp. 22-32.

[139] 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.

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

[141] Donald Trump announced his presidential candidacy on 16 June 2015. See: Time Staff, "Here's Donald Trump's Presidential Announcement Speech," Time, 2015, https://time.com/3923128/donald-trump-announcement-speech/.

[142] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 24-26.

[143] On social media statistics during the 2016 US presidential elections, see also: Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 14-33.

and WikiLeaks' notification of Hillary Clinton's sale of weapons to ISIS had 789,000.[144] In total the IRA's Facebook accounts may have reached 29 million US citizens and an estimated 126 million in total.[145] The IRA had also purchased some 3,500 ads some of which were used to organise rallies often in support of Trump and against Clinton.[146]

Between 10 March and 7 April 2016, the RF GRU, the Intelligence Directorate of the Ministry of Defence, targeted at least 109 Clinton campaign staffers, including the email account of campaign chairman John Podesta,[147] with 214 individual phishing emails. The GRU targeted Hillary Clinton's (private) email account at least two times in March, but the available data show that she did not fall for the password reset trick. Between 15 March and 11 April 2016, the GRU also hacked into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and on 18 April, of the DNC.[148] In total, the GRU stole hundreds of thousands of documents from the compromised email accounts and networks.[149]

The GRU hacks began to fuse with earlier RF disinformation operations in which the hacking of a target was combined with the release of sensitive data – or compromising material (kompromat).[150] The front organisations that were set up in the years before the Clinton and DNC hack were now used as outlets to disseminate compromising files,[151] complemented with Guccifer 2.0 and DC Leaks. The latter was registered on 19 April 2016.[152]

[144] 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. 9.

[145] The United Muslims for America Facebook account claimed to have more than 300K followers, Being Patriot over 200K. By 2017 Twitter accounts of Trump supporters such as @jenn_abrams and @Pamela_Moore13 claimed to have 70K followers each. In 2018 Twitter had identified 3.814 accounts (many bots) affiliated to the IRA reaching 1,4 million people. See: Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 26-28; 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. P. 1649; United States House of Representatives, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," Permanent Select Committee on Intelligence, n.d., https://intelligence.house.gov/social-media-content/.

[146] 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." pp. 7-11 & 40. The ads are available on: https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.; see also: Nina Jankowicz, *How to Lose the Information War - Russia, Fake News, and the Future of Conflict* (I.B. Tauris, 2020). pp. 2-9.

[147] Mohamed Helal, "On Coercion in International Law," *SSRN Electronic Journal*, no. 475 (2019). pp. 9-10.

[148] The hacks were performed by the GRU units 26165 and 74455 using X-Tunnel malware. Infiltrating the DNC might not have been a genuine hack. Some DCCC employees were authorised to access the DNC network. See: Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. pp. 79-81; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 36-38.

[149] United States District Court, Indictment (United States v Netyksho) (2018). pp. 2-3.

[150] Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information / Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity (Forthcoming)*, 2019, 1–29. p 14; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp 41-48; Efrony and Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice." pp. 609-611; Thomas Rid, "How Russia Pulled Off the Biggest Election Hack in U.S. History," *Esquire*, 2016.

[151] Such as Yemen Cyber Army, Cyber Berkut, Fancy Bears Hack Team, and @ANPoland see: Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." pp. 3-4.

[152] United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 13-14.

As of June 2016 the GRU released stolen Clinton campaign and (as of late July 2016) DNC documents through DC Leaks and Guccifer 2.0.[153] The release of the documents continued from 15 June to 18 October 2016, often in small batches to generate a sustainable impact,[154] and was intensified reaching a larger audience via non-RF actors such as Julian Assange's WikiLeaks, the retweeting of IRA posts by US opinion-leaders including the Trump campaign team,[155] and US and international journalists covering the DNC Leaks.[156]

RF-affiliated agents did not only oppose presidential candidate Clinton. Competing Republicans for the presidential primaries, including Ted Cruz, Mitt Romney and Marco Rubio were also targeted. Democrat Bernie Sanders, on the other hand, Clinton's democratic challenger in the primaries, was supported.[157] On 19 July 2016, the Republican National Convention nominated Donald Trump and running mate Mike Pence as Republican candidates for the 2016 elections. On 26 July 2016, the Democratic National Convention determined that Hillary Clinton was their presidential candidate, with Tim Kaine as vice-president, but not before the leaking on 22 July of some 20,000 emails outlining that the supposedly neutral DNC favoured Clinton over Sanders.[158] This revelation forced the DNC Chair, Wasserman Shultz, to resign.[159]

The team supporting Trump had been in contact with RF-affiliated or former Soviet States' officials for a variety of reasons.[160] Russian investors had sought contact with Trump's business organisation since 2013 for reasons of building a Trump Tower in Moscow. But also the Trump campaign team had been in contact with investors since late 2015/early 2016;[161] Trump's team was also triggered by the Russian suggestion that they had in their possession 30,000 emails of candidate Clinton containing 'dirt'[162] and finally contact was made, also with the RF Ambassador to the US, to refine future US-RF relations.[163]

[153] Guccifer initially was identified as a Romanian virtual persona but was later attributed to the RF GRU. 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. p. 154; Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019). pp. 116-124.

[154] E.g. the 7 October 2016 response by Wikileaks to the Access Hollywood incident which undermine candidate Trump. See: Helal, "On Coercion in International Law." pp. 14-15.

[155] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 33-35.

[156] Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." pp. 5-6.

[157] 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." pp. 34-37.

[158] 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; Ido Kilovaty, "The Democratic National Committee Hack: Information as Interference," *Just Security*, 2016.

[159] Helal, "On Coercion in International Law." pp. 13-14; Rid, "How Russia Pulled Off the Biggest Election Hack in U.S. History."

[160] Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. p. 121.

[161] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 67-75.

[162] The Trump team was interested in these emails by Clinton stemming from private accounts. Julian Assange suggested to have these mails, which commenced the liaison between Wikileaks and the Trump Team. See: Mueller. pp. 52, 80-81.

[163] Mueller. pp. 159-161.

On 7 October 2016 the so-called 'Access Hollywood' incident occurred. In this broadcast, candidate Trump claimed that due to his status he could treat women in inappropriate ways.[164] The incident was largely nullified by the Wikileaks dissemination of the Podesta emails hours later, containing onerous materiel undermining the political integrity of Clinton.

On that same day, 7 October, the US government officially accused the RF of intending to interfere with the US election process.[165] On 29 December 2016, a more technical elaboration was provided of these malicious Russian Cyber activities.[166]

Finally, on 8 November 2016, Donald Trump was elected 45th President of the US with 304 electoral votes against 227 for Democrat Hilary Clinton. The Republican party representative, Trump, received 46.1% of the popular vote against Clinton's 48.2%. President-elect Trump took office on 20 January 2017.

The campaigns in the run-up to the elections were divisive and dominated by activities to 'support the presidential campaign of Donald Trump and weaken Hillary Clinton's, and to undermine public faith in the U.S. electoral process and the democratic system'.[167]

Late in 2016 President Obama, before the transfer of the presidency, took actions against the RF cyber operations aimed at the US election, which 'harm U.S. interests' and are 'in violation of established international norms of behavior'.[168]

On 6 January 2017 the Office of the Director of National Intelligence released a report mentioning a Russian campaign to influence the election, with the aim to 'undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency' and it was assessed that 'the Russian Government developed a clear preference for President-elect Trump'.[169] In May 2017 a Special Counsel Investigation started, conducted by Robert Mueller, to assess the Russian interference in the 2016 Elections and possible links between the Trump campaign team and the Russian government. The Mueller Report, ending the investigation in March 2019, concluded that there was a clear and

[164] Mueller. pp. 20-21 & 58-59; Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information." pp. 156-157; Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. pp. 120-121.

[165] DHS, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security," *Department Of Homeland Security* , 2016, 1–2.

[166] DHS & FBI, "Grizzly Steppe – Russian Malicious Cyber Activity," *Jar-16-20296*, 2016.

[167] William Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States," *Michigan Journal of Race and Law* 24, no. 2 (2019). p. 200.

[168] Office of the Press Secretary, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harrassment," 2016.

[169] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 2017. p. ii.

systematic Russian preference for candidate Trump, but did not establish 'that members of the Trump campaign conspired or coordinated with the Russian government in its election interference activities'.[170]

On 16 February 2018 an indictment was issued against the IRA et al. and 13 of its employees,[171] and on 13 July 2018 another one was issued against 12 GRU operatives accused of violating national legislation by hacking the Clinton campaign team, the DNC and the DCCC, and releasing these stolen documents via DC Leaks and Guccifer 2.0.[172]

4.3.2. The objective and strategic narrative

Research and literature on the 2016 presidential election,[173] bear out that the aim of the 2016 RF influence campaign targeting the US presidential elections was to undermine public faith in the US democratic process,[174] to 'sow discord in American politics and society',[175] more specifically, to 'sow distrust and discord and lack of confidence in the voting process and the democratic process',[176] and to denigrate Secretary Clinton and harm her electability and potential presidency'.[177]

The RF's long-term narrative is to promote the prevalence of strong authoritarian systems over feeble liberal democracies.[178] The narrative is to countervail the Western idea that authoritarian regimes have a tendency to corrupt. The RF rationale is that all systems are fallible,[179] as – from the RF point of view – became evident after the 2016 Panama-paper[180] and release of (RF hacked) compromising medical information about US athletes after the

[170] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 1-2.

[171] United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32.

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

[173] Including Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

[174] 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. 186.

[175] 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." p. 4.

[176] 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. 35, quoting former-Homeland Security Adviser Lisa Monaco.

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

[178] As underlined in a 2019 interview: Lionel Barber and Henry Foy, "Vladimir Putin Says Liberalism Has 'Become Obsolete,'" Financial Times, 2019, https://www.ft.com/content/670039ec-98f3-11e9-9573-ee5cbb98ed36.

[179] 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. 27-28; Andreĭ Soldatov and Irina Borogan, *The Red Web : The Kremlin's Wars on the Internet*, First Edit (New York: PublicAffairs, 2017). pp. 313-316; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." p. 1.

[180] The 'panama papers' refers to set a 2,5 Terabytes leaked documents in the *Süddeutsche Zeitung* on 3 April 2016 about offshore bank accounts and private financial information on wealthy persons and organisations. The offshore accounts

so-called McLaren report had accused RF athletes of State-dictated use of doping during the 2014 Sochi Olympics,[181] revealing the hypocrisy of the Western political elite.[182] In line with that rationale, RF had a strong focus on Clinton who portrayed herself as a person of high integrity and part of the political elite. The RF simultaneously supported Trump who was not representing the existing political establishment and could be a democratically chosen leader with an authoritarian style.[183] The 2016 elections were aligned with an existing RF strategic narrative,[184] and it stands to reason that no new narrative for the 2016 elections was created.[185]

The 2016 election can be seen as a culmination of efforts that have started years earlier.[186] Shires argues that RF has used influence operations in Northern Africa and the Middle East as probes of the effectiveness of their instruments that would later be used in the run-up to the US presidential election.[187] Likewise, the hacks into the German Chancellor's website in January 2015 and into the French television network TV Monde in April 2015 can be seen as precursors.[188] In the US itself, the RF influence operations - affecting the 2016 presidential elections – may well have started as early as 2014.[189]

Russian interference in the US presidential election made use of both hard- and soft-cyber operations.[190] Hard-cyber elements are, first, the attacks on the cyber-infrastructure via

are often used to purposes of i.a. tax evasion. See: International Consortium of Investigative Journalists, "The Panama Papers: Exposing the Rogue Offshore Finance Industry," ICIJ, 2016, https://www.icij.org/investigations/panama-papers/.

[181] Richard H. McLaren, "WADA Investigation of Sochi Allegations," 2016.

[182] DFRLab, "# PutinAtWar : WADA Hack Shows Kremlin Full-Spectrum Approach."; Booz Allen Hamiltion, "Bearing Witness: Uncovering the Logic behind Russian Military Cyber Operations," *Booz Allen Hamilton*, 2020. p. 28; Russian MFA, "Leaks: 25 Athletes Used Doping with '@WADA_ama' Knowledge & Cover-up. Only 1 Russian, but 5 Brits, 10 Americans.," Twitter, 2016, https://twitter.com/RussianEmbassy/status/776343061504860161.

[183] Maarten Rothman, "On the Instrumentality of Soft Power; or Putin Against Democracy Promotion," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017*, ed. Paul A.L. Ducheine and Frans P.B. Osinga, 2017, 39–52. p. 43; Zygar, "Why Putin Prefers Trump."

[184] Karin von Hippel, "Axis of Disruption : Chinese and Russian Influence and Interference in Europe," 2020. p. 3.

[185] Soldatov and Borogan, *The Red Web : The Kremlin's Wars on the Internet*. p. 337.

[186] Rid, "How Russia Pulled Off the Biggest Election Hack in U.S. History."

[187] James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," *Journal of Cyber Policy* 4, no. 2 (2019): 235–56. p. 248.

[188] Soldatov and Borogan, *The Red Web : The Kremlin's Wars on the Internet*. p. 322; Jean Baptiste Jeangene Vilmer, "Lessons from the Macron Leaks," in *Hacks, Leaks and Disruptions*, ed. Nicu Popescu and Stanislav Secrieru, 2018. p. 8.

[189] 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. 3; Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." pp. 9-11; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 14.

[190] Aside from influence techniques via other domains, or executing espionage operations. An example of the former is the infiltration of Maria Butina into the NRA. See: Jens David Ohlin, *Election Interference: International Law and the Future of Democracy* (Cambridge University Press, 2020). p. 24; United States Department of Justice, "Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States," Office of Public Affairs, US DOJ, 2018, https://www.justice.gov/opa/pr/russian-national-charged-conspiracy-act-agent-russian-federation-within-united-states.

attempts to hack online voting systems.[191] The data in the logical layer of cyberspace was compromised. The Senate Committee on Intelligence found that at least 21 US States were targeted by RF attempts to scan data, gain access in a malicious way or attempt to access voting related websites. In a few US States attempts were made to delete or alter voter registration data.[192] On the other hand, there were no indications that election infrastructure was destroyed or manipulated, or that 'votes were changed, vote-tallying systems manipulated, or that any voter registration data were altered or deleted'.[193] Second, RF hackers from the APT 28, unit 26165 of the GRU have been identified gaining access to the DNC and later also penetrating the DCCC network.[194] This hack is further elaborated in § 4.3.4. as it is the precursor of wider soft-cyber activities including the leaking of prejudicial information.

Moreover, virtual personae were created to spread private, manipulated or falsified content.[195] RF agents masquerading as Americans manipulated social media accounts and identities.[196] The soft-cyber influence operation, which is the focus of this case, used cyberspace as a vector to execute disinformation tactics aiming to deepen social divisions as elaborated below.

4.3.3. Framing the narrative

The RF campaign narrative was aimed at undermining public faith in the democratic process, amplifying political polarisation, and delegitimising the electoral process. In the framing of the anti-liberal democratic narrative, the 2016 election and the path towards it, starting from 2014, was used as the event required to triangulate the narrative with socially divisive issues (such as race, immigration, police violence and the right to bear arms),[197] and heuristics of

[191] Diresta et al., "The Tactics & Tropes of the Internet Research Agency." p. 4; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." pp. 2-3.

[192] 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. 12-20. RF activities were related to penetrated voter registration database, viewed multiple database tables, and accessed voter registration records.

[193] United States Senate Committee on Intelligence. p. 38, though the Committee mentions that the insight of the Senate Committee and the intelligence community into this is limited.

[194] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 36-40; Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 10; Helal, "On Coercion in International Law." pp. 9-15.

[195] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 27.

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

[197] Lily H. Newman, "Russia Is Learning How to Bypass Facebook ' s Disinfo Defenses," *Security*, 2020. The Second Amendment of the US Constitution was adopted in 1791 and reads: "A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed."

the audiences, attempting to set up audiences against each other and/or against the national government,[198] even supporting contradictory frames in order to create confusion.[199] Framing this narrative in the context of the elections therefore went hand in hand with the promotion of 'disunity, discontent, hopelessness, and contempt of others, all aimed at sowing societal division',[200] in line with the overall anti- 'liberal democracy'-narrative.

To operationalise the narrative targeting the US presidential election, the framing focused on two avenues that were distinct in intent though inextricably linked in effect: discrediting Clinton and subsequently supporting Trump.[201] The RF framing did not necessarily follow party lines but did utilise anti-establishment sentiments and growing distrust in State institutions within society.

On the one hand the goal was to discredit Clinton, harm her chances of success, and diminish her electability and potential presidency,[202] based on her long-standing anti-Russian activities and posture,[203] in particular as Secretary of State,[204] as well as to promote a false illusion of the integrity of the American political elite.[205] The RF frame against Democratic candidate Clinton amplified her lineage with the old-boys-network, invoking the anchoring-, confirmation- and stereotyping bias, and fuelling the anti-establishment sentiments of large parts of the US audience.[206] During the run-up to the elections Clinton was therefore not only up against Trump, but also against the Russian anti-establishment

[198] Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 71-75; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 25.

[199] There were specific topics and key words per groups of the audience such as veterans, police support, patriotic, anti-Muslim for the conservatives; or the inequality, poverty, disproportional incarnation and police violence for Afro-Americans, but also geographically in the Heart of Texas identity versus the United Muslims of America in Texas. See: 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. 19 & pp. 23-25; and the 'themes' as listed in Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 11-13.

[200] 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. 32.

[201] Elswah and Howard in a research on RT argue paraphrase a former RT employee stating that 'RT seemed pro-Trump only because it criticized Hilary Clinton but, in reality, the channel would have supported any candidate running against her' in Elswah and Howard, "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)." P. 631; See also Helmus, "Social Media and Influence Operations Technologies: Implications for Great Power Competition." p. 155; S. Shane and M. Mazzetti, "The Plot to Subvert an Election," *The New York Times*, September 20, 2018.

[202] 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. 4; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." p. 1.

[203] David E. Sanger, "The Hawk on Russia Policy? Hillary Clinton, Not Donald Trump," *The New York Times*, October 20, 2016.

[204] Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 186; David E. Sanger, *The Perfect Weapon : War, Sabotage, and Fear in the Cyber Age* ([S.l.]: Scribe, 2018). p. 103.

[205] Making use or underscoring sentiments as illustrated in Peter Schweizer, *Clinton Cash: The Untold Story of How and Why Governments and Businesses Helped Make Bill and Hillary Clinton* (Harper, 2015).

[206] Aligned with or amplifying Trump's rhetoric, see: Trevor Hughes, "Trump Calls to 'Drain the Swamp' of Washington," USA Today, 2016, https://eu.usatoday.com/story/news/politics/elections/2016/2016/10/18/donald-trump-rally-colorado-springs-ethics-lobbying-limitations/92377656/.

frame supporting Clinton's fellow-Democrat Sanders.[207] Making extensive use of social media, the RF 'sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election'.[208] Starting in March 2016, numerous ads were published on social media platforms, allegedly sponsored by the RF-affiliated entities, with the aim to undermine Clinton's record with respect to her role in the attack on the US consulate in Benghazi, but also to her dismissive position towards religious factions.[209] The frame was intended to influence voters to abstain from voting, or even to cast their vote on alternative options including Jill Stein of the Green Party, who also gained some RF support.[210]

On the other hand, the RF did not support candidate Trump because he was a Republican - other Republicans candidates were side-lined[211] - but rather due to his non-political background and his 'refreshing',[212] or at least less negative stance towards the Kremlin,[213] and his scepticism towards broad cooperations with traditional allies.[214] The frame surrounding Trump focused on anti-establishment sentiments, and growing distrust of existing institutions and media. It could be argued that the frame presented Trump as the non-establishment candidate who could revisit existing institutions and media. The goal of the pro-Trump frame was also meant to encourage citizens with conservative leanings (even those not interested in politics)[215] to vote, and if so, but not to vote for Clinton. In a

[207] Diresta et al., "The Tactics & Tropes of the Internet Research Agency." p. 9; Michael Chertoff and Anders F. Rasmussen, "The Unhackable Election: What It Takes to Defend Democracy," *Foreign Affairs* 98, no. 1 (2019). p. 159.

[208] 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.

[209] Helal, "On Coercion in International Law." pp. 10-15; United States House of Representatives, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements."

[210] United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election-Volume 5: Counterintelligence Threats and Vulnerabilities," vol. 5, 2020. pp. 803-810; Helmus, "Social Media and Influence Operations Technologies: Implications for Great Power Competition." p. 155.

[211] In effect, Ted Cruz, Marco Rubio and Jeb Bush, 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." p. 6.

[212] Jared Kushner (Trump Campaign team) paraphrasing Sergey Kislyak (RF Ambassador to the US), in: Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 106; See also the meeting of Putin with Western journalists later in time, on 1 June 2017, covering an array of topics. Putin stated that Trump was a straightforward person with a fresh vision. "The Latest: France Says No Trace of Russian Hacking Macron," *AP News*, June 1, 2017. At 4.30 pm.

[213] "Donald Trump's Statements on Putin/ Russia/ Fake News Media," *Lawfare*, 2020.; Zygar, "Why Putin Prefers Trump."; it can even be argued that Cruz was the initial preference of large Republican segments. Heather Timmons, "If Cambridge Analytica Is so Smart, Why Isn't Ted Cruz President?," Quartz, 2018, https://qz.com/1234364/cambridge-analytica-worked-for-mercer-backed-ted-cruz-before-trump/.

[214] Ashley Parker, "Donald Trump Says NATO Is 'Obsolete', UN Is 'Political Game,'" *The New York Times*, April 2, 2016.

[215] Philippe J. Maarek, "Politics 2.0: New Forms of Digital Political Marketing and Political Communication," *Trípodos* 1, no. 34 (2014): 13–22. p. 19.

highly bipartisan system this meant supporting candidate Trump,[216] thereby appealing to the 'partyism-heuristic' of American politics.[217]

The information the Trump campaign team required to generate frames was largely acquired via data harvesting techniques. The Trump campaign team, by way of then advisor Steve Bannon, vice president of the US branch of Cambridge Analytica,[218] allegedly obtained 50 million profiles which could be cross-referenced with Facebook data to build an algorithm that could determine and predict personality traits linked to voting behaviour.[219] Frames made by Cambridge Analytica for the Trump team associated the loss of jobs with Clinton's support for the NAFTA, linking actual social economic topics and problems to conditioned reflexes of the population related to the alleged elitist position of the Clinton family.[220] The frames could highlight Clinton's earlier support to the Iraq war, connecting her to that war, which was under scrutiny at that moment of the elections.[221]

The RF made use of and exaggerated existing division and sentiment of the US population. Though the Mueller 'investigation did not establish that members of the Trump Campaign conspired or coordinated with the Russian government in its election interference activities',[222] the subsequent disinformation and trolling campaigns appeared to coalesce with campaign themes as commenced or used by the Trump team. [223]

4.3.4. Cyber-related activities

Overall, the RF operation to influence the US presidential elections was more intense than that during the UK EU referendum.[224] The operation was well-prepared, longer in duration,

[216] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 4.

[217] Meaning: if they are for it, we are against it, see: Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, NED-New, Divided Democracy in the Age of Social Media (Princeton University Press, 2018). p. 263.

[218] Cambridge Analytica worked for the Leave.EU campaign during the Brexit (see: § 4.2.1) but earlier for the campaign of US Republican Senator Ted Cruz, see: Ido Kilovaty, "Legally Cognizable Manipulation," *Berkeley Technology Law Journal* 34 (2019). pp. 466-467; Patrick Svitek and Haley Samsel, "Ted Cruz Says Cambridge Analytica Told His Presidential Campaign Its Data Use Was Legal," The Texas Tribune, 2018, https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/.

[219] Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 191-192; Carole Cadwalladr and Emma Graham-Harrison, "Revealed : 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach Interruption," *The Guardian*, March 17, 2018.

[220] Helal, "On Coercion in International Law."

[221] Paul Lewis and Paul Hilder, "Leaked : Cambridge Analytica ' s Blueprint for Trump Victory," The Guardian, 2018, https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

[222] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 5.

[223] the Trump campaign team had links with Russian agents, as alluded in the Mueller Report, and Mueller's testimony before the House Judiciary Committee. See part IV of Mueller. pp. 66 ff; "Transcript of Robert S. Mueller III's Testimony before the House Judiciary Committee," *The Washington Post*, (2019).

[224] 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. 5; Lucas Kello, *The Virtual Weapon and*

saw a clear RF initiative and made extensive use of supportive hard-cyber operations:[225] These included attempts to gain access to voting computers and voter registration databases,[226] but also an intense hacking operation into the network of the Clinton campaign team, the DNC and the DCCC, which preceded the (soft-cyber) leaking of prejudicial information.[227]

In March and April 2016, APT 28 (unit 26165 or Fancy Bear),[228] associated with the military intelligence service GRU, targeted Clinton campaign staffers with individual phishing emails - fraudulent messages disguised as legitimate requests in an attempt to acquire sensitive data, in this case credentials such as usernames and password to gain access to the victims' networks, or cause the recipients to download malware that enabled the sender to gain access to an account or network.[229] Initially some 90 spear phishing mails were sent to accounts related to hillaryclinton.com, and later, as of 15 March 2016, the Google email accounts of the Clinton campaign team were targeted.[230] After gaining access, the GRU unit 26165 obtained tens of thousands of emails from the Clinton Campaign employees.[231]

The spear phishing attempts on the Clinton campaign team extended to their dnc.org and dccc.org account since some employees either still had such an account as they had formerly worked for the DNC or DCCC, or Clinton employees were authorised to access the DNC and DCCC network. Apart from the spear phishing, access to the DNC and DCCC networks was accomplished via the VPN connection between the DNC and DCCC network,[232] and

International Order (New Haven [CT] SE - xi, 319 pages ; 25 cm: Yale University Press, 2017). p. 226.

[225] Hacks, spear phishing but also encrypted keys, data listening devices, see also: Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns."p. 5; Martin and Shapiro identified 13 cyber-related attacks from the Russian Federation, 3 from Iran and 3 from an unknown origin. Diego A. Martin and Jacob N. Shapiro, "Trends in Online Foreign Influence Efforts," *ESOC Publications*, 2019. pp. 40-46.

[226] 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 ff.

[227] United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 2-3. See also: Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 11-18.

[228] Fancy Bear is also known as ATP 28 or Unit 26165. The Mueller report refers to Military Units 26165 and 74455 which are part of the GRU. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 36-37; Greenberg argues that Unit 26165 is Fancy Bear, while 74455 is Sandworm (or Voodoo Bear), Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. p. 269; United States District Court, Indictment (United States v Andrienko) "Sandworm," 20–316. pp. 1-2; Initially the assessment was that the GRU (APT 28) and FSB (APT 29 or Cozy Bear) both acted during the DNC and DCCC hacks, this was later reassessed to the above mention two units from the GRU. See also: Efrony and Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice." p. 609; Renée Diresta and Shelby Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019" (Stanford, 2019). pp. 70-72.

[229] United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 6-8. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." Note 112 pp. 35-36; Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." pp. 235-236; Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 28; "Cyberspace Solarium Commission," 2020. p. 137.

[230] In total appr. 214 mails were sent to 109 campaign employees. See Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." pp. 4-5; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 35-36. Helal, "On Coercion in International Law." pp. 9-10.

[231] Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 188-189.

[232] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 38.

by impersonating political fundraising platforms using the actblues.com domain.[233] The GRU modified the DCCC website and on both the DNC and DCCC website the X-Agent and X-Tunnel malware were installed. The X-Agent hacking tool allowed unit 26165 to gather data (file directories, log keystrokes, take screenshots) from the infected computers, while X-Tunnel made it possible to move documents via an encrypted channel from the DCCC/ DNC computers to GRU-controlled computers outside the DCCC and DNC networks.[234] The malware could search the networks for documents containing specific words, including Hillary, DNC, Cruz, or Trump.[235] After gaining access the GRU obtained credentials of DCCC and DNC members and donators, and they pilfered approximately 70 gigabytes of data.[236]

Though the hard-cyber intrusions into the ICT infrastructure were persistent and well documented, the soft-cyber influence operation during the 2016 US presidential election might have had more impact. The influence operation consisted of the leaking of the stolen data, spreading disinformation and mal-information, and supporting – or defamation of - the principle candidates. All these forms of (soft) cyber-related activities were used following the two overarching frames which crystallised in the run-up to the elections;[237] supporting Trump e.g. by targeting the more conservative segment of the electorate to vote for Trump, and on the other hand, by undermining Clinton e.g. by pressing African-Americans to abstain from voting or to support the anti-establishment candidate Sanders.[238]

The leaking of sensitive information started as of 19 April when confidential documents from the DNC, the DCCC, and the email account of John Podesta, chairman of Hillary Clinton's 2016 presidential campaign,[239] were leaked online by the virtual persona of DC Leaks, mainly the DC Leaks Facebook and Twitter account (@dcleaks_). Data were also shared via email through the GRU operatives that were in contact with reporters and US officials,[240]

[233] Martin and Shapiro, "Trends in Online Foreign Influence Efforts." pp. 41-42.

[234] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 38-39. United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 10-11.

[235] United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 10-11.

[236] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 36-41. While the GRU sister unit 74455 (aka 'Sandworm') attempted to gain access to infrastructure related to the administration of the elections e.g. boards of elections, or U.S. companies providing software. See also: Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. pp. 260-262.

[237] Supporting Trump might not have been the RF aim from the start of the campaign. The core was to support a candidate which would cause mayhem in the political establishment, preferably be pro-Kremlin. The RF also were against Clinton due to her earlier engagements with RF. See also: Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 33-36.

[238] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 25-27; Diresta et al., "The Tactics & Tropes of the Internet Research Agency." p. 9.

[239] 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.

[240] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." p. 42.

while fictitious US virtual persona (e.g. 'Jason Scott') were created to further promote and whitewash the leaked data.[241]

On 14 June 2016 the DNC announced that it had been hacked by Russian government actors. In response, the Guccifer 2.0 virtual identity was created, allegedly a lone Romanian hacker responsible for the intrusion into the Democratic networks.[242] Guccifer 2.0 shared, including via WordPress-hosted blog, 2.5 gigabytes of DCCC data, Black Lives Matters files and donor registration with journalists and bloggers covering the elections, but also with lobbyists and US officials.[243] To increase the dissemination of the leaked information the GRU shared data with Wikileaks as of June 2016.[244] On 22 July, three days before the Democratic National Convention, Wikileaks (in the US indictments referred to as 'organisation 1'[245]) shared more than 20,000 emails and documents obtained from the DNC network.[246] Between 7 October and 7 November 2016 Wikileaks released more than 50,000 documents and mails from the Podesta hack.[247] Wikileaks never mentioned the source of the data nor disclosed the role of Guccifer in the release of data. The lack of transparency regarding the source of the leaks was further exacerbated by a supporting disinformation campaign claiming that the leak was 'an inside job'.[248]

The leaks targeted Clinton and the Democrats, not the Republicans, pointing towards a specific intent to undermine the legitimacy of the Clinton candidacy and damage her integrity. The campaign of leaking sensitive information had significant media impact,[249] generating several scandals and headlines about Clinton and her staff as it revealed that the DNC was biased against the Sanders campaign and had a clear preference for, and close ties

[241] 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.

[242] Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*. p. 78; United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 14-15.

[243] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 42-44; United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 14-17.

[244] Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents."p. 10; Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0." p. 1. On 22 July 2016, more than 19.000 DNC email were released in Wikileaks; Soldatov and Borogan, *The Red Web : The Kremlin's Wars on the Internet*. pp. 322- 323, who in this sense speak about the unstoppable 'data haemorrhage'. Guccifer 2.0 is most likely a virtual persona of GRU officials, see: Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 42-44.

[245] United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 3 ff.

[246] See: @WikiLeaks & WikiLeaks, "Hillary Clinton Email Archive," WikiLeaks, 2016, https://wikileaks.org/clinton-emails/.

[247] United States District Court, Indictment (United States v Netyksho), 1:18-215. pp. 18-19.

[248] In August 2016 Wikileaks tried to sow confusion by stating that Seth Rich, a Clinton campaign employee who was killed on 10 July 2016, was the source of the leak. See: Cailin O'Conner and James O. Weatherall, *The Misinformation Age: How False Beliefs Spread* (New Haven [CT]: Yale University Press, 2019). pp 162-165; Diresta and Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019." p. 82; United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election-Volume 5: Counterintelligence Threats and Vulnerabilities." p. 220.

[249] And resulted in the indictment of 12 GRU officials in February 2018, and a criminal complaint in September 2018 against Elana Khusyaynova, see: United States District Court, Indictment (United States v Netyksho), 1:18-215.; United States District Court, Criminal Complaint (United States v Khusyaynova) (2018).

with the Clinton campaign.[250] Furthermore, it revealed Clinton's paid speeches at Goldman Sachs,[251] alluding to her connectedness to the American gentry and business network.[252] The hack, and subsequent publication via Wikileaks, appeared to be politically motived and might have been commenced as a tit-for-tat activity,[253] after the dissemination of the 2016 Panama Papers,[254] which were embarrassing for Putin, the 2016 McLaren reports on the doping affair surrounding the RF athletes in 2014,[255] sanctions against the RF after the annexation of Crimea,[256] and the generic anti-Kremlin stance of the US government.[257]

The disinformation campaign revolved around factual, false and fabricated content and followed two paths: discrediting Clinton with the emphasis on her attachment to the existing political system; and supporting the presidency of Trump as a newcomer who could be used to address distrust in the existing political system and attached media. The focus on Clinton and Trump instead of on the Democrats and the Republicans made the campaign after the primaries very personal.

Divisive societal topics were fit into the frames and used during disinformation and trolling campaigns. Specific groups were micro-targeted with on-line political campaigns, based on their gender, geographic location, and political ideology.[258] From conservatives, Muslim Americans to LGBT, voters received bespoke messages, both in content and form,[259] with the intent to manipulate or radicalise their behaviour; or political adverts with the aim to 'cause divide along racial, religious and political ideologies'.[260] Of the societal issues - such

[250] Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0." p.1.

[251] Soldatov and Borogan, *The Red Web : The Kremlin's Wars on the Internet*. p. 319.

[252] Helal, "On Coercion in International Law." pp. 14-15. Helal mentions that Clinton is described as an elitist, establishment figure detached from 'normal' Americans.

[253] Shane and Mazzetti, "The Plot to Subvert an Election."

[254] Paul Radu, "Russia: The Cellist and the Lawyer," *OCCRP*, April 26, 2016.; Anders Åslund, "Russia's Interference in the US Judiciary" (Atlantic Council (Eurasia Center), 2018). p. 10; Soldatov and Borogan, *The Red Web : The Kremlin's Wars on the Internet*. pp. 312-319.

[255] Diresta and Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019." pp. 75-79; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." p. 1; 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. 31-34; Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (2019): 212–34. p. 222.

[256] See e.g. United States Department of the Treasury, "Ukraine-/ Russia-Related Sanctions," 2020, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions.

[257] 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. 32-33.

[258] Federica; Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections," 2018. p. 21; 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. pp. 158-165.

[259] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." Pp. 19-20. Memes, comedy or music streaming was used to target Young voters.

[260] Dutt, Deb, and Ferrara, "'Senator, We Sell Ads': Analysis of the 2016 Russian Facebook Ads Campaign." p. 166.

as immigration, healthcare, police violence, and gun control - race was the one most used by the RF framing and scripting efforts to divide the country.[261]

The disinformation campaign regarding Clinton resembled a defamation attack,[262] antagonising her as a person and not as a political figure, dissipating the difference between disinformation and trolling. The examples of fabricated content and falsified news are numerous.[263] Clinton was linked to child trafficking known as 'pizzagate', again aimed at undermining her integrity and moral reputation.[264] She was also accused of selling weapons to ISIS and held responsible for the 2012 killing of US Ambassador Stevens in Benghazi.[265] All the themes in the disinformation campaign alluded to the ingrained bias of large groups of people that Clinton could not be trusted. The themes confirmed the bias. But there were more subtle examples. The Obama administration allegedly treated US veterans poorly - in comparison to refugees - and since both Obama and Clinton were Democratic politicians, the topic was anchored suggesting that Clinton too would act accordingly.[266]

Trump, on the other hand, was supposedly supported by the Pope.[267] The frame linked to this element of disinformation is that the Pope was said to support Trump, not since the former agreed with him, but because the FBI would not prosecute Clinton on criminal charges suggesting that in-crowds of the current the political system protect each other,[268] again alluding to idea the Clinton was not to be trusted.[269] The intended result is to create an illusion of papal support for Trump (linking him to the Christian values of Republicans), while the integrity and credibility of Clinton is undermined and consequently voters,

[261] Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States." pp. 208-209; Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 8-11; 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. 6; Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 7; Diresta and Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019." pp. 57-61; Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 11.

[262] Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 8; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 77.

[263] Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 10; 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.

[264] Marc Fisher, John W. Cox, and Peter Herman, "Pizzagate: From Rumor, to Hashtag, to Gunfire in D.C.," *The Washington Post*, December 6, 2016.

[265] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 13.

[266] Howard, Kelly, and François. pp. 19-20.

[267] Other false or misleading news topics were: "Hilary voted for the Iraq War, Donald Trump opposed it – Crooked Hilary voted for the war in Iraq as senator for New York. Bad judgement!"; or "Hillary supports NAFTA, She will ship jobs oversea", see also: Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook," BuzzFeed News, 2016, https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

[268] O'Conner and Weatherall, *The Misinformation Age: How False Beliefs Spread*. p. 3.

[269] It was even suggested that Clinton was responsible for making Seth Rich 'disappear', a Clinton modus operandi that had happened before in the past. See: Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 69-72; O'Conner and Weatherall, *The Misinformation Age: How False Beliefs Spread*. pp. 162-165.

traditionally inclined to vote for the Democratic party, will shift to other parties or abstain from voting altogether.[270]

The RF cyber-related activities often reached the US population beyond the Clinton- Trump dichotomy, and though often labelled as disinformation, most topics entail junk news going beyond the intent of a disinformation campaign to sow discord and could better be classed as a trolling campaign.

The trolling campaign aimed to further polarise the existing (or growing) divisions within the US society fuel the discourse with slander, hate speeches and discrimination, with the aim to undermine the electoral process by micro-targeting specific groups. IRA campaigns for African-Americans including the 'Blacktivists', 'BM' or 'BlackMatters' with a focus on African-American cultural and racial issues and police brutality,[271] addressed their latent distrust in (and alleged bias of) the media and government institutions[272] and in the electoral system, with the aim of dissuading them from casting their vote.[273] Apart from the intrusions related to the Clinton campaign team and the DNC, the GRU also executed soft-cyber activities mainly to increase racial animus via the Michael Brown Memorial Facebook page,[274] and underscore police brutality, e.g. by creating the National Association Against Police Brutality (NAAPB).[275]

The RF agents (IRA) targeted far-right voters via social media, e.g. @March_for_Trump-Twitter account, but also via websites including Ending the Fed,[276] and fed them with conspiratorial, sensational and other junk news in order to make them more confrontational both on-

[270] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 19; Despite the dominant bipartisan political culture, there were numerous other presidential candidates, during the 2016 election, among them were Gary Johnson of the Libertarian Party, Jill Stein of the Green Party or Darrell Castle of the Constitutional Party. See: Federal Election Commission, "Official 2016 Presidential General Election Results," 2017.

[271] United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32. 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.

[272] Social media outlets used include Facebook (fb.com/blackmatters), Instagram (@blackmattersus), Twitter (@ blackmatters), Soundcloud, Tumblr, YouTube and Google+. See: Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 42-44; Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." pp. 19-21.

[273] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 3; Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 87-88.

[274] Michael Brown jr was an Afro-American who was shot by policeman Darren Wilson in Ferguson Missouri, after an altercation and after Brown fled. After a trail Wilson was not charged with any crime. John Eligon, "No Charges for Ferguson Officer Who Killed Michael Brown, New Prosecutor Says," *The New York Times*, July 30, 2020.

[275] Diresta and Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019." pp 57-61.

[276] Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook."Endingthefed.com (no longer on-line) and Endthefed.org or via the Twitter account @Endingthefed.

and off-line.[277] Making use of techniques such as 'astro-turfing',[278] the IRA was responsible for creating, generating or supporting grassroot themes such as 'Stop All Invaders', a clear reference to illegal immigrants. Likewise, the theme 'Being Patriotic' was all about support for the Second Amendment (the right to keep and bear arms), which inherently echoed the distrust in the political system. In Texas both the tags on the 'Heart of Texas'-Facebook page regarding 'Stop Islamization of Texas' and the 'United Muslims for America' were RF agent-borne.[279] To enhance the sentiments of distrust of the government and its institutions, following on the UK Brexit, a polarising theme was set up to suggest that Texas would split off from the US rather than then to continue in the current political system.[280] The fictitious 'Army of Jesus' was a carefully built up conservative social media group such as on Facebook, Twitter and Instagram, and after gaining momentum, it was propagated that Clinton was opposed to the ideas of the 'Army',[281] alluding to her lack of Christian values.[282]

The impact of these disinformation and trolling campaigns was increased by the use of false fronts, social media accounts to impersonate Americans[283] and by propagating political beliefs on opposing ends of the political spectrum, going so far as to organise rallies and protests through these accounts,[284] and not least by 'unwitting' journalists covering the topics without properly checking the facts.[285]

Political grooming was most visible in the advertisements on Facebook, purchased by the RF.[286] Though most adverts referred to divisive and inflammatory social issues pertaining to race, sexuality, gender identity, immigration and Second Amendment, some adverts contained direct references either to supporting Trump or discrediting Clinton, e.g. 'Hillary Clinton Doesn't Deserve the Black Vote', 'We cannot trust Hillary to take care of our veterans!' or 'Trump is our only hope for a better future!'[287] The political grooming was also

[277] United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32. pp. 21-23.

[278] Astro-turfing refers to corporate or State activities pretending to be grass root or peer-level initiatives, with the purpose of influencing the governmental agenda or policy, making (fraudulent) use of social media. See: Ohlin, "Election Interference: The Real Harm and The Only Solution." p. 5; Ohlin, *Election Interference: International Law and the Future of Democracy*. p. 22.

[279] Tim Lister and Clare Sebastian, "Stoking Islamophobia and Secession in Texas -- from an Office in Russia," *CNN Politics*, October 6, 2017.

[280] Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 69-72; And also called for the secession of California, see: Luis Gomez, "A Russian Twitter Bot Promoted California Secession, or Calexit," *The San Diego Union-Tribune*, November 2, 2017.

[281] 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." pp. 33-47.

[282] Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 71-72.

[283] Outsiders participating in a (foreign) political process but pretending to be insiders is what Ohlin calls 'the real harm' of election interference, see: Ohlin, "Election Interference: The Real Harm and The Only Solution." p. 16.

[284] Galante and Shaun, "Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." p. 10.

[285] Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." p. 6.

[286] Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 189.

[287] United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32. p. 50; United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S.

substantiated via the IRA retweeting of posts, and political rallying instigated by the IRA. The IRA, whose activities coalesced with the objectives of the Trump campaign team. The latter even forwarded IRA-borne Tweets[288] and indeed supported the rallies, though there is no evidence that the Trump team was aware the request to support came from foreign entities.[289]

Political grooming is not a one-sided activity. The Mueller report concluded that 'the evidence was not sufficient to support criminal charges' concerning collusion, nor 'to charge a criminal campaign-finance violation'.[290] Though the Trump team was interested in the spoils of the DNC and DCCC hacks which could undermine Clinton and support the Republican ticket, the Mueller report was inconclusive on whether the Trump team was aware of the DNC hack and potential dissemination of data;[291] or whether the Trump team was directly involved in initiating the GRU activities.[292] However, on the other hand, there had been contact between individuals of the RF government and the Trump campaign team.[293] It is even possible that during the 2016 US presidential elections the Trump campaign team pro-actively solicited and engaged RF support.[294]

4.3.5. Exploiting social media

The frames and scripts made for the 2016 US presidential elections were used to tackle the targeted audiences during the execution phase via cyber-related disinformation and trolling activities, either independently or supporting the leaking of sensitive information and political grooming operations. The cyber-related activities saw many variations on to the same theme of undermining Clinton's position and supporting Trump's, ranging from Clinton's supposed incapacity for public office; the supposed poor treatment of veterans by Obama and the prospect of yet another Democratic president; or safeguarding Christian values by, and the papal support for, Trump.

Election - Volume 2: Russia's Use of Social Media." p. 44;

[288] 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. 54.

[289] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 33-35. Trump, as a businessman also had ties with Russia related to real estate projects such as the Moscow Trump Tower- project see: pp. 67-75.

[290] Mueller. p. 9.

[291] Mueller. pp. 51- 66; Jensen, Valeriano, and Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." p. 221.

[292] The Mueller report does state that the Trump team was informed as of 25 April that the RF had discrediting information on Clinton, see: Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 88-89.

[293] Stephen Kotkin, "American Hustle: What Mueller Found - and Didn't Find - About Trump and Russia," Foreign Affairs, 2019, 1–32.; see also Part IV of volume I of Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 66-143.

[294] Ohlin, *Election Interference: International Law and the Future of Democracy*. pp. 191 ff.

Though these frames and subsequent disinformation and trolling themes do not reflect reality or causality and are largely false and fabricated, audiences may have perceived them to be true thought constant repetition and exposure. Messages become familiar after frequent repetition, and cyberspace - especially social media – is able to facilitate amplifying and magnifying the content of disinformation and trolling campaigns. Actors, including RF agents can reach and access vast foreign audiences at low prices of admission, and negligible levels of control.[295] Furthermore, cyber-related activities provide plausible deniability for the actor executing the activity.

During the 2016 US elections a multitude of RF actors were active on social media in amplifying and magnifying the frames using a multitude of cyber-related activities, to sow discord and increase political polarisation by exploiting divisive political issues on racial tensions and police brutality, and to undermine public faith in democratic institutions and, at the same time support the pro-Russian candidate Trump, meanwhile discrediting the political 'dynasties'[296] such as the Clintons and undermine Hillary's campaign. Not only the IRA, but also the GRU and its affiliated APT 28 were active on social media, sometimes in concert, but often separately.

In order to magnify the message, instead of using one outlet the RF agents engaged in cross-platform activity.[297] Different platforms, outlets and a multitude of accounts were used effectively including Twitter,[298] Instagram, YouTube, Facebook,[299] Reddit, Tumblr and to a lesser extent, Linkedin, Medium, Pinterest and Google, since the latter were ill suited for micro profiling.[300] Twitter, on the other hand was effective in creating the illusion of predictable behaviour. Ruck et al. conclude that a growth of 25,000 re-tweets per week would increase Donald Trump's poll numbers by one percent.[301] Though the impact of trolls (human agents) on Twitter should in general not be overrated, Russian trolls were very active regarding topics related to Clinton and Trump.[302] Moreover, according to Liberini, the on-

[295] 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. 15.

[296] Kotkin, "American Hustle: What Mueller Found - and Didn't Find - About Trump and Russia."

[297] 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.

[298] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 27: "the IRA Twitter data shows a long and successful campaign that resulted in false accounts being effectively woven into the fabric of online US political conversations right up until their suspension."

[299] Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." pp. 189 ff.

[300] 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." pp. 8-9; Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 22-28.

[301] Damian Ruck et al., "Internet Research Agency Twitter Activity Predicted 2016 U.S. Election Polls," First Monday, 2019, https://firstmonday.org/ojs/index.php/fm/article/view/10107/8049.

[302] Savvas Zannettou et al., "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web," *Arxiv*, 2019. Pp. 1 & 7.

line political campaign on Facebook was effective and especially favourable to Trump as the on-line campaign 'persuading Republican and moderate supporters to go to vote, and in swaying their votes towards Trump'.[303] Whether these resulted in swaying the elections is another matter,[304] not least since the mechanisms behind on-line political advertising are still elusive.[305]

While exploiting social media RF agents made use of false virtual identities impersonating Americans, along with extensive use of bots, trolls and political advertisements, though the latter were marginal in number.[306] During the election campaign the RF reached millions of US voters[307] by sending out 61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets and by purchasing 3,400 Facebook and Instagram advertisements.[308] The peaks in posts and adverts coalesced with key events during the election such as the primaries, national debates or election day. The exploitation of social media by making use of bots was primarily intended to influence and fuel extreme political opinions. Far-left and far-right extremists in the political landscape produced 25 to 30 times more messages than regular mainstream political accounts.[309] Bots, automated social media accounts, were used to amplify messages and increased the spreading, while trolls, which in general are human operators, micro-targeted specific groups in chat rooms, blogs or on-line forums, with the purpose to mislead the audiences behind the virtual persona and provoke responses on-line or in reality.

All in all, RF influence operations exploited social media (which coalesced with US on-line political activities) via multiple media, with high volume and speed using automation, algorithms, and big-data analytics to manipulate public life.[310] This so-called computational propaganda 'encompasses issues to do with so-called 'fake news', the spread of

[303] Liberini et al., "Politics in the Facebook Era. Evidence from the 2016 US Presidential Elections." p. 37.

[304] Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (2017): 211–36. p. 232, Allcot suggests that given the fact that every new campaign advert changes the votes with 0.02 percent, the consolidated percentage for all adverts is smaller than the margin of victory.

[305] Samuel Spies, "Election Interference," Media Well, 2019.

[306] 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. 7; Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 3; United States House of Representatives, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements."

[307] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." pp. 14-15; Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 192, Denton argues that the IRA adds reached up to 29 million Facebook users by 'liking' and 'sharing' content was viewed by least 126 million users.

[308] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." P. 3; Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 76 ff. Note: Howard & Kelly (2018), but also DiResta et al. (2018), Ruck (2019) or Helmus (2020) make use of data provide to the US Senate Committee on Intelligence. Howard & Kelly are not a corroboration of the Senate Report.

[309] 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. 10.

[310] Linvill & Warren even speak about 'industrialised political warfare' in this sense, see: Darren L Linvill and Patrick L Warren, "Troll Factories: The IRA and State-Sponosred Agenda Building," *Working Paper*, 2018. p. 13.

misinformation on social media platforms, illegal data harvesting and micro-profiling, the exploitation of social media platforms for foreign influence operations, the amplification of hate speech or harmful content through fake accounts or political bots, and clickbait content for optimized social media consumption'.[311]

4.3.6. Generating effects

The Russian influence operations did not stop after the 2016 election, nor after the exposure to the IRA or the indictment of GRU. In fact, the activity on social media increased after the 2016 election day,[312] though it shifted from Facebook and Twitter to Instagram as the main social media platform, thereby using other forms of communication (images and memes) addressing a younger audience.[313] The decline in the use of Facebook was most likely due to changes in Facebook policy to limit the spread of fabricated and false news.[314] Again, in the 2018 mid-term elections RF influence operations peaked,[315] albeit with moderate effect, on the one hand because of measures deriving from the lessons learnt and,[316] on the other, since the population was no longer off-guard. After the 2016 election numerous investigations started, including by Special Counsel Robert S. Mueller III, which might have led to dynamics that fuelled partisanship rather than focus on an effective response towards the 2016 and future Russian interference. The Trump administration denied that the RF had interfered with the 2016 election, hence ruling out that the Trump campaign team could be associated, let alone had colluded, with the RF.[317] Partisan issues further denied the adoption of legislation to protect the elections and related infrastructure.[318]

[311] Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 39.

[312] 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; Howard, Kelly, and François, "The IRA, Social Media and Political Polarization in the United States, 2012-2018." p. 3. The Russian originated Facebook posts covered topics such as the Syrian missile strike in April 2017, the bombing of the ISIS tunnels and the US tax reform plan.

[313] Diresta et al., "The Tactics & Tropes of the Internet Research Agency." pp. 96-98.

[314] Hunt Allcott, Matthew Gentzkow, and Chuan Yu, "Trends in the Diffusion of Misinformation on Social Media," *National Bureau of Economic Research*, 2019. pp. 2-3.

[315] Ben Nimmo et al., "# TrollTracker : Facebook's Midterm Takedown," *DFRLab*, November 13, 2018.; Sean Gallagher, "Report : US Cyber Command Took Russian Trolls off Line during Midterms," *Ars Technica*, 2019.

[316] Several agencies (FBI, ODNI, US Cyber Command) set up election security initiatives to counter foreign interferences (FITF) or to act against information operations (NDAA), see also: Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." pp. 2-3; Lahmann, "Information Operations and the Question of Illegitimate Interference under International Law." p. 214; Helmus, "Social Media and Influence Operations Technologies: Implications for Great Power Competition."Brett Holmgren and Benjamin Haas, "A Model for Countering Foreign Disinformation and Interference in Elections," *Just Security*, 2020.; Laura Rosenberger, "The Real Threat of Foreign Interference Comes after Election Day," *Foreign Affairs*, 2020.

[317] Chertoff and Rasmussen, "The Unhackable Election: What It Takes to Defend Democracy." p. 160. A reaction which would not be objected by the RF as it was in line with the overall aim to cause strategic confusion.

[318] Graham Brookie and Emerson T. Brooking, "The Senate Created a Playbook to Counter Foreign Influence. Then It Did the Opposite," *Just Security*, 2020.; Holmgren and Haas, "A Model for Countering Foreign Disinformation and Interference in Elections."

Compared to the 2016 elections, the interference from outside actors during the 2020 presidential election appeared to be more subtle, or less unexpected. But the RF influence was not negligible. A pre-election assessment bore out that interference was present,[319] characterised by trolls that spread hyper partisan topics and 'highly networked accounts' able to propagate and share messages fast.[320] The notion that foreign electoral interference is less obvious does not imply that RF agents are not active in the US.[321] On 15 March 2021 the Office of the Director of National Intelligence released a report on the 2020 presidential election, mentioning that there was no indication that electoral infrastructure or software was meddled with – hence no hard-cyber activities -, but there were indications that RF executed an influence operation to 'affect US public perception of the candidates as well as advance Moscow's long-standing goals of undermining confidence in US election processes and increasing socio-political division among the American people.[322] On 15 April 2021 the Department of Treasure adopted sanctions against several RF entities and individuals for their role in interfering with and undermining the 2020 US presidential election.[323]

Richey argues that an effect of the Russian influence operations is an increase in cynicism in domestic politics,[324] distrust in government institutions and a deeper bipartisan and societal rift regarding divisive topics such as the right to bear arms, race, religion and police violence. The citizens are 'primed to doubt the outcome'[325] of elections and maybe even about the integrity of the democratic electoral system.[326] The attack on the Capitol on 6 January 2021 echoes this effect, and while world leaders were appalled by the incident, 'the violence fit(s) neatly into the Kremlin's narrative of a crumbling American democracy.'[327]

[319] Camille François, Ben Nimmo, and C. Shawn Eib, "The IRA CopyPasta Campaign: Russian Accounts Posing as Americans on Instagram Targeted Both Sides of Polarizing Issues Ahead of the 2020 Elections," 2019.

[320] William Marcellino et al., "Foreign Interference in the 2020 Election," 2020. pp. 9-12.

[321] RF was also allegedly responsible for the widespread intrusions affiliated with the security breaches of SolarWind, a company providing software to a multitude of US governmental agencies, corporation, hospitals and universities, see: Herbert S. Lin, "Reflections on the SolarWinds Breach," *Lawfare*, 2020, 1–4.; David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *The New York Times*, January 2, 2021.; Georgi Kantchev and Warren P Strobel, "How Russia's 'Info Warrior' Hackers Let Kremlin Play Geopolitics on the Cheap," *The Wall Street Journal*, January 2, 2021.

[322] Office of the Director of National Intelligence, "Foreign Threats to the 2020 US Federal Elections," 2021.

[323] United States Department of the Treasury, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," 2021.

[324] Mason Richey, "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation," *Asia Europe Journal* 16, no. 1 (2018): 101–13. p. 109.

[325] Rosenberger, "The Real Threat of Foreign Interference Comes after Election Day."

[326] Alina Polyakova, "The Kremlin's Plot Against Democracy: How Russia Updated Its 2016 Playbook for 2020," *Foreign Affairs*, 2020.; Kello, *The Virtual Weapon and International Order*. p. 223.

[327] "Live Updates: Joe Biden Is Certified as the 46th President of the United Senate and House Vote to Certify Biden ' s Victory," *The New York Times*, January 7, 2021.

4.3.7. Concluding remarks

In sum, the RF executed influence operations in the US, during the 2016 US election, started as early as 2014 and lasted until after the elections. The campaign to affect and undermine the US presidential election appears to have been deliberately prepared, executed and exploited by the RF. Compared with the influence operations during the US presidential elections, the UK EU referendum appeared to have been a piece-meal operation by the RF, supporting domestic actors.

The 2016 US presidential election provided an opportunity to exploit an existing anti-liberal democracy narrative. In the run-up to the election the RF independently scripted tailor-made frames aiming to sow discord, polarise groups and undermine the political process.

In executing the frames, the RF used socially divisive topics to support presidential candidate Trump and discredit his antagonist Clinton. However, the US election not only fuelled the traditional bipartisan division between Democrats and Republicans, it also scattered the traditional Democratic support due to a strong anti-establishment frame which not only buoyed up Trump, but also promoted Clinton's Democratic opponent Sanders.[328] Moreover, the prospect of the election of another representative of the US political establishment (Clinton) was used to dissuade African and Latin-Americans from voting.

The RF influence operations were elaborate and comprised many aspects of the traditional Active Measures and reflexive control doctrine. The main hard-cyber activities in the run-up to the 2016 election were the intrusions into the ICT systems of the Clinton campaign team, the DNC and the DCCC. Though most attention went to these hacks, the more 'pernicious intervention'[329] taking place was an elaborate soft-cyber influence operation including the leaking of sensitive and prejudicial information, disinformation campaigns and trolling. The political grooming campaign was intense and extensive but partly conducted outside the remit of cyberspace.

The leaking of prejudicial information worked well in the US presidential election, although this will not always be the case as a rule. Many hacks will provide useless data. In the US Case however, leaking information, not only boosted the defamation attacks to discredit Clinton, but also added to the general confusion about the genuine nature of the data since the source was not revealed or purposely disputed, concealing the originator.

The disinformation campaigns in the run-up to the elections was or became very personal, transforming them into trolling operations highlighting and depending the existing

[328] Ball, *Post-Truth: How Bullshit Conquered the World*. pp. 84-87.

[329] Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States." pp. 178-179.

division between groups, including the racial divide, rather than creating discord. The trolling operations relied heavily on the heuristics of audiences injected both by the Trump campaign team (supported by SCL/Cambridge Analytica)[330] and by the RF frames during their influence operations.

Exploiting social media to boost the content shared via the cyber-related activities proved very effective during the 2016 election. The RF multi-platform influence operation made full use of the attributes of cyberspace to magnify and amplify the frames executed via the disinformation and trolling campaign, repeating the content of messages with the purpose to create an illusion of truth.

Section 4.4.: The 2017 French Presidential Election

Moi, je suis la candidate du pouvoir d'achat,
Vous, vous êtes le candidat du pouvoir d'acheter[331]

Une campagne ne se passe jamais comme prévu[332]

4.4.1. The path to the presidential election

Though France lacks the bipolar political culture, that exists in the UK and the US, Socialist and Republican presidents have alternated since the emergence of the 5th Republic.[333] The 2017 French presidential election, however, 'did not follow the expected course'.[334] In the second round of the presidential election, neither the socialists nor the republicans were represented;[335] the two largest parties were the far-right *'Front National'* with Marine Le Pen, and the novel political movement *'(La République) En Marche'* led by Emmanuel Macron.

[330] Though the constellation changed overtime, SCL, Aggregate IQ and Cambridge Analytica are interrelated compagnies with SCL as the parent enterprise for the two subsidiaries. See also: Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. pp. 96-100.

[331] LePen to Macron (paraphrasing) during the presidential debate on 3 May 2017. See: Cyril Simon, "Débat Macron-Le Pen : 10 Phrases Choc Pour Un Bras de Fer Sous Haute Tension," *Le Parisien*, 2017.

[332] Gérard Courtois, *Plan de Campagne: La Saga Des Élections Présidentielles* (Perrin, 2017). p. 7 subtitle to Introduction.

[333] Established on 4 October 1958 by De Gaulle, who became the first president. See also: Jocelyn Evans and Gilles Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?," French Politics, Society, and Culture (Cham, Switzerland: Palgrave Macmillan, 2018). pp. 17-18.

[334] Evans and Ivaldi. p. 1.

[335] Raymond Kuhn, "Expect the Unexpected: The 2017 French Presidential and Parliamentary Elections," *Modern and Contemporary France* 25, no. 4 (2017): 359–75. pp. 367-369.

France has a rich political landscape with numerous political parties representing the traditional political schools of thought (liberal, social, communist), but also more nationally-oriented affiliations (Gaullist, Republicans). In recent decades new parties have emerged reflecting popular concerns about the environment or immigration. During the period between 2007 and 2017 in which Sarkozy (UMP)[336] and Hollande (*Parti Socialiste*) were successive presidents of France the landscape of French political parties become increasingly polarised and fragmented.[337]

While the polarising and fragmentary developments left a gap in the political centre,[338] the 2017 elections were dominated by populist tendencies, distrust in traditional parties and the popular call for political renewal.[339] This, in turn, favoured party candidates during the primaries that did not represent the political mean.[340] In 2017, most political parties had elected front persons that tended to accentuate distinctive positions of the party that were less moderate. The quasi-Gaullist party *Debout La France* of Dupont was Eurosceptic; Mélenchon's *La France Insoumise* (LFI) was a (far) left Eurosceptic party; Le Pen's *Front National* (FN) was a far-right anti-EU movement. Hamon, the new leader of the Socialist Party (PS) was a representative of the left-wing and Eurosceptic segment of the PS and was critical of incumbent PS president Hollande.[341] Surprisingly, Fillon was elected candidate for the Republicans (the new name for the UMP) instead of Juppe,[342] a moderate and popular politician.[343] Though *Les Républicains* is a conservative-liberal party with Gaullist origins, their presidential campaign was affected by a political scandal involving privileges granted to Fillon's wife, Penelope.[344] This provided an opportunity for new parties, most of all Macron's pro-EU *En Marche!* and Mélenchon's LFI, the latter receiving 19.1% of the votes in the first round.[345]

On 4 February 2017, RF-affiliated Sputnik news agency published articles suggesting that Macron was a US agent supported by a 'gay' bank lobby, in addition to innuendo regarding

[336] Jocelyn Evans and Gilles Ivaldi, *The 2012 French Presidential Elections: The Inevitable Alternation* (Palgrave Macmillan, 2012). p. 40. The 'mainstream Right' UMP – *Union pour un Mouvement Populaire* – is a 2002 fusion between the Gaullist RPR (established by Chirac) and the Liberal Democratic party, at the time Chirac was president.

[337] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" pp. 28-40.

[338] Evans and Ivaldi. p. 41.

[339] Kuhn, "Expect the Unexpected: The 2017 French Presidential and Parliamentary Elections." p. 364, Kuhn calls this the 'twin processes of dégagisme and renouvellement', referring to getting rid of the old system/ renew the political system; Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" pp. 46-47.

[340] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" p. 60.

[341] Evans and Ivaldi. pp. 49-56.

[342] Kuhn, "Expect the Unexpected: The 2017 French Presidential and Parliamentary Elections." p. 363.

[343] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" p. 1.

[344] Kuhn, "Expect the Unexpected: The 2017 French Presidential and Parliamentary Elections." pp. 365-366; Gerard Davet and Fabrice Lhomme, "La Tragédie de La Droite, Épilogue : La Grande Débâcle de François Fillon," Le Monde, 2019, https://www.lemonde.fr/politique/article/2019/02/08/la-tragedie-de-la-droite-epilogue-malheur-aux-vaincus_5420792_823448.html.

[345] Oscar Barrera et al., "Facts, Alternative Facts, and Fact Checking in Times of Post-Truth Politics," *Journal of Public Economics* 182 (2020). p. 4.

Macron's private life and sexual orientation.[346] While Republican candidate Fillon was under attack in France for 'Penelopegate',[347] RT and other media outlets continue to spread news about Macron instead, connecting him to Jewish bankers and portraying him as Islam protagonist.

In the first round of the French presidential election, on 23 April 2017 no candidate obtained a majority after which a run-off was required between the two best scoring candidates Macron and Marine Le Pen, with 24.1 and 21.3% of the popular vote, respectively.

The disinformation, or rather trolling campaign continued and on 3 May 2017, the day of the public debate between Macron and Le Pen, fake documents were shared via the #MacronGate hashtag on the US-based platform 4chan, suggesting Macron had an overseas back account. Though the post was shared via Twitter, the document proved to be fabricated.[348]

In addition to the disinformation and trolling campaign, the Macron campaign team had been targeted via spear phishing and email spoofing[349] since December 2016 and at least five email accounts of Macron team employees were hacked.[350] Documents were not leaked until 5 May 2017, just hours before the 44-hour period of electoral silence started.[351] The documents were posted on message boards such as Pastebin.com, Archiv.org and 4chan.org, and later disseminated via mainstream social media platforms including Twitter and Wikileaks.[352] It is suggested that the hack and leak originated from the main RF intelligence services, most likely the GRU's unit 74455 also known as Voodoo Bear or Sandworm,[353] though the French government has never attributed the attack to the RF or any other State.[354]

[346] Jeangene Vilmer, "Lessons from the Macron Leaks." p. 76; Sputnik News, "Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests," *Sputnik*, February 4, 2017.

[347] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 6-9. See also Philip N. Howard et al., "Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter?," *Comprop Data Memo*, no. May (2017): 1–5. Most Tweets in the period between 13-19 March (the sample area) where related to Macron. p. 3

[348] Jeangene Vilmer, "Lessons from the Macron Leaks." p. 76; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 9-10.

[349] Feike Hacquebord, "Two Years of Pawn Storm," *Trendlabs Research Paper*, 2017. pp. 11-13.

[350] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" pp. 99-100.

[351] Lasting from Friday midnight (5 May 24.00) to election day on Sunday (7 May 20.00), see: "Interdiction de Diffuser Des Sondages Les Samedi 6 et Dimanche 7 Mai 2017," *CNCCEP*, 2017.

[352] Emilio Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election," *First Monday* 22, no. 8 (2017). Under: Introduction; The further distribution via mainstream platforms is called 'whitewashing'. Mika Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling," 2017. p. 4; Jeangene Vilmer, "Lessons from the Macron Leaks." p. 77.

[353] United States District Court, Indictment (United States v Andrienko) "Sandworm," 20–316. pp. 15-16; Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. pp. 315-316; Martin Untersinger, "Les Preuves de l'ingérence Russe Dans La Campagne de Macron En 2017," *Le Monde*, December 6, 2019.; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 18-20.

[354] Boris Toucas, "The Macron Leaks : The Defeat of Informational Warfare," *CSIS Briefs*, 2017. p. 1; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 23; Matt Tait, "The Macron Leaks: Are They Real, and Is It Russia?," *Lawfare*, May 2017.

The leaking of sensitive or private information by the combined effort of RF-affiliated and pro-Russian alt-right activists, had a limited effect, due to the (poor) timing and the non-sensitive content of the retrieved hacked data.[355] On 6 May the French electoral commission urged media and voters not to rely on the leaked documents.[356]

A final instrument that was used was the funding of Le Pen's Front National through RF banks and the support her party – but also other pro- Russian candidates e.g. Mélenchon - received via RF media outlets, 4chan and other alt-right internet outlets.[357]

On 7 May 2017, Emmanuel Macron won the French presidential election with 66.1% in the second round and became 8th president of 5th Republic. Vilmer argues that the foreign operation to influence the French presidential elections had failed. One of the reasons for this could be that France had the opportunity to learn from influence operations during the 2016 UK EU referendum and US presidential election.[358]

4.4.2. The objective and strategic narrative

Targeting the French presidential election falls within the remit of the anti- EU, anti-NATO and anti- liberal democracy narrative of the Russian Federation (RF).[359] Similar to the UK EU referendum case, the French presidential election was an opportunity to advocate Russian discomfort with the attitude of the Western States and their posture of liberal democratic superiority.[360]

The French political landscape saw stark political differences towards the EU, NATO and the RF. During the French election, the Front National of Marine Le Pen was openly opposed

[355] Stefan Soesanto, "The Macron Leak That Wasn't," *European Council of Foreign Relations*, 2017.; 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). pp. 15-16.

[356] The electoral commission is called the Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle (CNCCEP). See: "Recommandation Aux Médias Suite a L'Attaque Informatique a Été Victime L'Équipe de Campagne de M. Macron," CNCCEP, 2017, http://www.cnccep.fr/communiques/cp14.html.; Jeangene Vilmer, "Lessons from the Macron Leaks." pp. 80-81.

[357] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" p. 100; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 24-25; Natalie Nougayrède, "Spectre of Russian Influence Looms Large over French Election Officials Are on Alert for Campaign Meddling," 2017.

[358] Jean Baptiste Jeangene Vilmer, "Successfully Countering Russian Electoral Interference," *CSIS Briefs*, 2018, 1–6. pp. 1-2; Jeangene Vilmer, "Lessons from the Macron Leaks." p. 75; Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." pp. 9-10; Toucas, "The Macron Leaks : The Defeat of Informational Warfare." p. 2; Martin Matishak, "NSA Chief : U.S. Warned France about Russian Hacks before Macron Leak," *Politico*, May 2017.

[359] Barber and Foy, "Vladimir Putin Says Liberalism Has 'Become Obsolete.'"

[360] Or as Aaltola states "autocracies have come to view democratic appeal as a destabilising threat to themselves, as a driver behind internal democratic movements and colour revolutions" which would also partially account for RF interest in influencing the outcome of the election. Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling." p. 3.

to EU sanctions against Russia,[361] opposed the EU and NATO and supported a right-wing nationalistic rhetoric which not only corresponded with some of the RF points of view but would also weaken Western unity. Not only Le Pen was negative about the EU and NATO, also Francois Fillon (*Les Républicains*, centre-right) and Jean-Luc Mélenchon (LFI, far-left wing) assumed that position.[362] Conversely, Emmanuel Macron advocated the EU and was supportive of the EU sanctions against the RF,[363] and had ousted Sputnik and RT from any Macron campaign venue.[364]

The divisive political landscape could have been conducive to the RF to discredit Macron and support Le Pen in seeking 'to drive wedges between western democracies',[365] underscoring the anti-liberal democracy narrative. The RF influence operations, which coincided with the (non-State) 'Alt-right' activists[366] and the Le Pen campaign did therefore resemble an *argumentum ad hominem* or personal attack on Macron.[367]

France is a critical though crucial member of NATO and, together with Germany, a key pillar of the EU especially after the secession of the UK. France is a respected democracy and one of the main players in the Western alliance. Furthermore, France hosts one of the largest far-right political parties, Le Pen's Front National. Unlike the population in the UK, the French are not resentful against Russia and there are even strong cultural, political and economic relations, though the current Russian regime is unpopular in France.[368] From an RF strategic perspective, France appears to be an interesting target for an influence operation,[369] not least since there appeared to be similarities with both the UK and the US governmental and societal constellation.

The foreign electoral interference, as assumingly executed by RF, involved forms of hard-cyber and soft-cyber activities. The hard-cyber operations entailed hacks on both political parties and media institutions, most notably the Macron campaign team, as highlighted in

[361] Since March 2014, the EU has applied restrictive measures (sanctions)) against the RF in response to the crisis in Ukraine (i.e. the annexation of the Crimean peninsula), see: European Council, "EU Restrictive Measures in Response to the Crisis in Ukraine," accessed June 24, 2021, https://www.consilium.europa.eu/en/policies/sanctions/ukraine-crisis/.

[362] Kuhn, "Expect the Unexpected: The 2017 French Presidential and Parliamentary Elections." p. 364; Polyakova et al., "The Kremlin's Trojan Horses." pp. 7-8.

[363] Booz Allen Hamiltion, "Bearing Witness: Uncovering the Logic behind Russian Military Cyber Operations." p. 33.

[364] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 36; Reuters, "Emmanuel Macron's Campaign Team Bans Russian News Outlets from Events," *The Guardian*, April 27, 2017.

[365] Nougayrède, "Spectre of Russian Influence Looms Large over French Election Officials Are on Alert for Campaign Meddling."

[366] Alt-right is an international virtual community. The US branch of the Alt-Right movement was allegedly involved in the Macron Leaks. See: Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." pp. 2 ff.

[367] Denton, "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." p. 209; Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" p. 115. An ad hominem attack is instigated by the motivation of the originator targeting the opponent in person, and not whether the rational argument is right or wrong.

[368] Polyakova et al., "The Kremlin's Trojan Horses." p. 11.

[369] Nougayrède, "Spectre of Russian Influence Looms Large over French Election Officials Are on Alert for Campaign Meddling."

§ 4.4.4.[370] During the hack data, documents and personal files were retrieved from the ICT systems of the Macron campaign team. Though there was a hard-cyber operation against TV5 Monde in 2015,[371] there were no publicly reported hard-cyber operations directed at the election infrastructure, possibly due to the fact that France abandoned nearly all electronic (or on-line) voting.[372]

The influence operations during the 2017 French presidential election was primarily a soft-cyber operation, supported by a hack on the Macron campaign team. During the soft-cyber operation the most pertinent activities were the leaking of information and execution of trolling activities.

4.4.3. Framing the narrative

Operationalising the RF narrative means applying the generic anti-EU and anti-liberal democracy theme to the specific situation of the French election and the French audience. The narrative needs to be triangulated with socially divisive topics and preferences and cognitive or social heuristics of the population, all revolving around the elections.

In the years preceding the 2017 elections, France saw numerous political scandals and highly divisive topics pitting domestic groups against each other; or against the Hollande government.[373] On 7 January 2015 Michael Houellebecq released his book 'Soumission', a controversial novel fictitiously set against the background of the 2022 presidential election, in which the so-called Muslim party, supported by centre-right and centre-left parties as a counterweight to candidate Marine Le Pen, won the elections.[374] Though fictitious, the book underscores the opportunistic move of French politics, away from French culture and values.[375] But above all, it raises the topic of the influx of immigrants from former French colonies,[376] and the problems with far-right and far-left populist ideologies. On that same day

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

[371] Cairan Martin, "Cyber-Weapons Are Called Viruses for a Reason: Statecraft and Security in the Digital Age" (King's College London, 2020). p. 7; Laura Daniels, "How Russia Hacked the French Election," Politico.eu, 2017, https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

[372] Jeangene Vilmer, "Successfully Countering Russian Electoral Interference." p. 3; Assemblee Nationale, "Commission Des Lois Constitutionnelles, de La Législation et de l'administration Générale de La République (XIVe Legislature)," 2017. p. 14

[373] The Hollande presidency was not popular, the reason why Hollande (unprecedentedly) did not seek a second term. See: Kuhn, "Expect the Unexpected: The 2017 French Presidential and Parliamentary Elections." pp. 360-362.

[374] Michel Houellebecq, Soumission (Flammarion, 2017).

[375] John Rosenthal, "Houellebecq's 'Submission': Islam and France's Malaise," *World Affairs* 178, no. 1 (2015): 76–84. pp. 79-80; also Macron was accused of that, see: Yves Jego, "Emmanuel Macron et Le Reniement de La Culture Française Consommatrice de Produits Culturels Mondialisés," Figaro, 2017, https://www.lefigaro.fr/vox/politique/2017/02/06/31001-20170206ARTFIG00209-emmanuel-macron-et-le-reniement-de-la-culture-francaise.php.

[376] Rosenthal, "Houellebecq's 'Submission': Islam and France's Malaise." p. 79; Sylvain Bourmeau, "Scare Tactics: Michel Houellebecq Defends His Controversial New Book," *The Paris Review*, January 2015.

the satirical newspaper *Charlie Hebdo* was targeted by the Kouachi brothers, allegedly members of Al Qaeda. More attacks followed, including on a Jewish supermarket on 9 January, now by a person claiming to be a member of ISIS. In the run-up to the elections political scandals emerged, such as the so-called 'Penelopegate', revealed by another satirical newspaper, *Le Canard Enchaîné*,[377] claiming that presidential candidate Fillon employed his wife, Penelope, as an 'aid', for which she received a handsome salary without actually working. Other incidents concerned Macron's misplaced statements on the French colonial period when in Algeria,[378] on the fictitious employments of assistants to Le Pen in the European Parliament,[379] or on the ongoing discourse on secularisation, the so-called *laïcité*,[380] especially when related to the rights of Muslim minorities.[381]

Though numerous topics dominated the French media and societal discourse, none of these sentiments were exploited, neither by RF agents nor by French political parties or political movements. Consequently, the RF influence operation could not follow the lead or the guidance of domestic campaigns highlighting divisive topics, let alone generate a clear frame itself. The Front National started the 2017 campaign with an anti-immigration frame, but during the campaign shifted to economy, social issues and attacking the EU in order to change the image of the party.[382] Though the framing of the EU as the source of economic malaise is more aligned with the RF strategic narrative to polarise French society, the frame was not fully aligned with the sentiments of the general public. The RF, therefore, was not able to fully grasp the genuine French political topics, namely the economic gloom, terrorism (alluding to the role of Islam), the role of the EU and 'voter disenchantment with traditional governing parties'.[383]

The foreign influence operation that targeted Macron's campaign team was most likely a mix between Russian elements and elements of the so-called 'foreign legion' of American alt-right activists who were in support of Le Pen's,[384] which might have hampered consistent

[377] Toucas, "The Macron Leaks : The Defeat of Informational Warfare." p. 3; AFP, "Penelope Fillon Aurait Reçu 900 000 Euros Au Total, Selon « Le Canard Enchaîné »," *Le Monde*, January 31, 2017.

[378] AFP, "En Algérie, Macron Qualifie La Colonisation de «crime Contre l'humanité», Tollé à Droite," *Le Monde*, February 15, 2017.

[379] Gerard Davet and Fabrice Lhomme, "Le FN Au Cœur d'une Enquête Pour Fraude," *Le Monde*, March 10, 2015.

[380] Laïcité, refers to the constitutional principle of secularism which discourages religious expressions in public life, and is embedded in the first Article of the 1958 French Constitution: *"La France est une République indivisible, laïque, démocratique et sociale. Elle assure l'égalité devant la loi de tous les citoyens sans distinction d'origine, de race ou de religion. Elle respecte toutes les croyances. Son organisation est décentralisée."*

[381] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" p. 181; Ben Smith, "The President vs. the American Media," *The New York Times*, 2020.

[382] Barrera et al., "Facts, Alternative Facts, and Fact Checking in Times of Post-Truth Politics." pp. 4-5.

[383] Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" pp. 151 & 180; Paul Belkin, "France's 2017 Presidential Election: In Brief," *Congressional Research Service*, 2017. p. 4.

[384] Toucas, "The Macron Leaks : The Defeat of Informational Warfare." p. 1; Harkinson, J., Inside Marine Le Pen's Le Pen's "Foreign Legion" of American Alt-Right Trolls: 4channers and other "meme warriors" are battling for France's far-right

framing. The overall narrative of RF was to achieve strategic confusion while the alt-right was seeking to endorse Le Pen. In the bipartisan situation as was the case during the 2016 US election, these aims would coalesce. However, in the 2017 French elections they did not. France does not have a bipartisan political landscape despite the fact that in the second round of the presidential election two remaining candidates competed. The RF could therefore have supported several relatively pro-Kremlin candidates, not only Le Pen, whose ideology coalesced with RF interests. Finally, where in the 2016 US presidential election the pro-Russian candidate blended with the anti-establishment candidate, this was not the case in France. Though Le Pen was a political outsider, owing to her father her family name is part of the political establishment,[385] whereas Mélenchon, but especially Macron could, be seen as relative newcomers.[386]

Moreover, it is possible that the RF but also the alt-right activists were not able to fully comprehend the cognitive and social heuristics of French society and politics, possibly made worse by the lack of language skills and knowledge of political context and culture.[387] Many posts on social media by the alt-right community, referring to socially divisive topics, such as migration, anti-Islam and anti-globalisation were in the English language. These posts were hardly shared in France mainly due to 'cultural clumsiness' of the originators and the French public's reticence about reading post in English.[388]

The result is that the RF framing focused on the person of Macron, thus obliquely supporting pro-Kremlin candidates, including Le Pen, while neglecting many cross references to socially divisive topics and heuristic preferences of the French population. Consequently, the cyber-related activities did not fuel French sentiment or audience preferences.

presidential candidate, on *Mother Jones*, 3 May 2017. https://www.motherjones.com/politics/2017/05/marine-le-pen-alt-right-american-trolls/

[385] Marine Le Pen is the daughter of Jean-Marie Le Pen who founded Front National in 1972. Marine Le Pen succeeded her father in 2012 as leader of the party. The granddaughter of Jean-Marie Le Pen, Marion Maréchal was also member of FN between 2010-2017. In 2018 the name of the party was changed to *Rassemblement National*. See i.a.:

[386] Philippe J. Maarek and Arnaud Mercier, *La Présidentielle Chamboule-Tout. La Communication Politique Au Prisme Du « dégagisme »*, Éd. L'Harm (Paris, 2018). p. 7. Newcomer (or outsider) is a relative term, though Macron never held an elected position, he attended the École Nationale d'Administration (ENA), and joined the cabinet of Hollande and later as minister of economy under former Prime Minister Vals.

[387] On the perception of French culture, see also: Jego, "Emmanuel Macron et Le Reniement de La Culture Française Consommatrice de Produits Culturels Mondialisés."

[388] Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 112; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 29; DFRLab, "'Macron Antoinette': Alt-Right Targets France," *Atlantic Council*, 2017.; Isabella Hansen and Darren J. Lim, "Doxing Democracy: Influencing Elections via Cyber Voter Interference," *Contemporary Politics* 25, no. 2 (2019): 150–71. p. 162.

4.4.4. Cyber-related activities

The main cyber-related activities in the run-up to the 2017 French elections were the leaking of sensitive information, trolling, political grooming, and a limited domestic disinformation campaign.[389] The (hack and) leak campaign, supported by a trolling and disinformation campaign, was an attempt to undermine the candidacy of Macron, while the political grooming was an attempt to support pro-Kremlin candidates including Le Pen.

Two days before the second round of the presidential elections, 9 GB of data from the Macron campaign team was leaked to the press.[390] The leaking of data itself – known as the 'Macron Leaks'[391] - was the culmination of a targeted campaign that had started late 2016.

The 'leak' was preceded by a 'hack', an intrusion into the ICT systems of the Macron campaign team. In January 2017 the team had already confirmed that they were the victim of phishing attempts. Though the French government has never accused the Russian Federation, others have attributed the attack to GRU-affiliated APT 28 (Fancy Bear), which is also likely to have been responsible for the US DNC hack.[392] In a later stage the hack was also attributed to the Sandworm APT, also a unit of the GRU.[393]

The Macron campaign team was targeted via seven spear phishing campaigns which addressed more than 100 email accounts of the team but also of affiliated politicians and French officials. The emails contained topics intending to lure the receiver into activating a fraudulent link, including email related to account lockouts, software updates or to sensational news (e.g. on terrorist attacks in the vicinity). One of the fraudulent links led to the instalment of software that enabled sharing of documents via communal Google

[389] Martin and Shapiro identify two foreign influence efforts both related to attacking Macron during the elections and linked to the leaks and anti-Macron propaganda. Martin and Shapiro, "Trends in Online Foreign Influence Efforts."pp. 31-32.

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

[391] Tait, "The Macron Leaks: Are They Real, and Is It Russia?"; Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." p. 106.

[392] Both the NSA and technology firm 'Trend Micro' have attributed the attempt to the GRU, see: Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure'.," Wired, 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.; Brattberg and Maurer, "Russian Elections Interference: Europe's Counter to Fake News and Cyber Attacks." p. 10; Patrick Tucker, "France's Macron Hack Likely By Same Russian Group That Hit DNC, Sources Say," Defense One, 2017, https://www.defenseone.com/technology/2017/05/frances-macron-hack-likely-same-russian-group-hit-dnc-sources-say/137636/.; Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 32; Eric Auchard, "Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group," *Reuters*, 2017.

[393] Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. pp. 360-361; United States District Court, Indictment (United States v Andrienko) "Sandworm," 20–316. pp. 15-16.

Doc, Drive or Dropbox applications.[394] These applications were set up specifically for this operation.[395]

Initially, between 12 and 26 April 2017, the GRU operatives shared some of the stolen documents with French individuals. Many of the documents shared on 3 and 5 May were edited on 27 April confirming the suspicion that they some had been tampered with.

On 3 May, just before the final debate between Macron and Le Pen, two (fabricated) documents were posted on 4chan, using a Latvian IP address.[396] The documents suggested that Macron had a secret overseas bank accounts in the Caribbean islands.[397] Le Pen referred to these leaked documents and emails during the final debate.

On Friday 5 May some 150,000 false and genuine emails, photos and documents from, or linked to, the hacked accounts of the Macron team were shared[398] hours before the electoral purdah – a 44-hours electoral silence before casting the ballot. The leaked emails were posted by user 'EMLEAKS' on the discussion board of PasteBin,[399] and via #MacronLeaks shared via 4chan, Wikileaks and placed on Twitter by US alt-right accounts including @ DisobedientNews and @JackPosobiec and retweeted some 47,000 times in three-and-a-half hours by real people and bots.[400]

The leaking campaign was invigorated by a disinformation campaign suggesting that, apart from the claim that Macron had secret overseas bank accounts, he was providing arms to ISIS,[401] and that his campaign was partially financed by Saudi Arabia.[402] Whereas the hack

[394] United States District Court, Indictment (United States v Andrienko) "Sandworm," 20–316. p. 15; But also other could data storage application were targeted, see: Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 11; Soesanto, "The Macron Leak That Wasn't."

[395] Such as 'onedrive-en-marche.fr' see: Hacquebord, "Two Years of Pawn Storm." p. 13; Lorenzo Franceschi-Bicchierai, "Russian Hackers 'Fancy Bear' Targeted French Presidential Candidate Macron," *Monsterboard*, April 2017.

[396] 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); Soesanto, "The Macron Leak That Wasn't." under 'chronicle of a hack foretold'.

[397] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 9.

[398] Kevin Limonier and Louis Petiniaud, "Mapping Cyberspace: The Example of Russian Informational Actions in France," in *Drums*, ed. Norman Vasu, Benjamin Ang, and Shashi Jayakumar (Singaoore, 2019), 49–60. p. 52; Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 2; Evans and Ivaldi, "The 2017 French Presidential Elections : A Political Reformation?" pp. 99-100.

[399] Hansen and Lim, "Doxing Democracy: Influencing Elections via Cyber Voter Interference." pp. 161-162.

[400] Ben Nimmo et al., "Hashtag Campaign: # MacronLeaks," DFRLab, 2017, https://medium.com/dfrlab/hashtag-campaign-macronleaks-4a3fb870c4e8.Jeangene Vilmer, "Information Manipulation: A Challenge for Our Democracies." pp. 108-109; Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 8 (MacronLeaks Bots and their Characteristics). Ferrara argues that 'out of 99,378 users involved in MacronLeaks, our model classified 18,324 of them as social bots, and the remainder of 81,054 as human users.'.

[401] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."

[402] Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making," *Council of Europe*, 2017. pp. 21-22; The Observers, "Debunked : Was French Candidate Macron's Campaign Financed by Saudi Arabia ?," France24, 2017, https://observers.france24.com/en/20170302-debunked-was-french-candidate-macron-campaign-financed-saudi-arabia.

into the Macron campaign team pointed to RF involvement, this becomes less obvious when assessing the leaking of information or the disinformation campaign. A study by Limonier et al. indicated three groups of Twitter accounts using the MacronLeaks hashtag: pro-Trump networks, writing in English;[403] the far-right French accounts; and finally, the Twitter accounts that were hostile to the far-right and often pro-Macron. Most of the accounts that opposed Macron were - albeit pro-Russian - French or American in origin.[404] Only 1.5% of all MacronLeaks-related Tweets originated from Russian platforms.

The apparent limited involvement by RF agents based on Tweets referring to the MacronLeaks could be caused by the fact that the hacked material did not 'reveal anything remotely damning to Macron'[405] or to the campaign. The hack as such might have created a scandal; the hacked information did not.[406] This could also be the reason why the hacked data, due to the lack of actual content, had been doctored before they were leaked.

This does not mean that the RF influence was marginal. The RF tried to influence the public debate in France first via Sputnik News and RT.[407] Furthermore, the RF was also active on Twitter, thereby making use of pro-Russian French or American alt-right accounts that actively relayed Russian media content, or via accounts that unwittingly used the argument of the Russian platforms. In this sense, Limonier et al. speak of a pro-Russian Twittersphere.[408] On 4chan and Discord, a meme of Macron was portrayed as a French (female) aristocrat, quoting: 'laisser les s'enriche'.[409] Macron was also linked to the unpopular President Hollande, suggesting that voting Macron meant another five years with Hollande.[410] Both frames address the anchoring heuristic linking Macron to the existing political elite or to the then unpopular incumbent who offered no solution to the economic problems of the country.

By focusing the cyber-related activities on a person rather than on themes, the activities resemble a trolling rather than a disinformation campaign.[411] It was suggested that Macron

[403] Approximately 32% of the Tweets in the research by Limonier and Petiniaud were in the English language, 61% was in French. Limonier and Petiniaud, "Mapping Cyberspace: The Example of Russian Informational Actions in France." pp. 56-57.

[404] Limonier and Petiniaud. pp. 56-58.

[405] Soesanto, "The Macron Leak That Wasn't." p. 3. One of the folders contained documents of Macron as 25-year-old student.

[406] James Shires, "The Simulation of Scandal : Hack-and-Leak Operations, the Gulf States, and U.S. Politics," *Texas National Security Review* Fall (2020). p. 27.

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

[408] Limonier and Petiniaud, "Mapping Cyberspace: The Example of Russian Informational Actions in France." pp. 51-52.

[409] Meaning: let's enrich ourselves. See: John Harkinson, "Inside Marine Le Pen's 'Foreign Legion' of American Alt-Right Trolls," Mother Jones, 2017, https://www.motherjones.com/politics/2017/05/marine-le-pen-alt-right-american-trolls/.

[410] Harkinson.

[411] Martin and Shapiro, "Trends in Online Foreign Influence Efforts." pp. 31-32.

had a relationship with his wife's daughter from a previous marriage and that he loved Yaoi,[412] in both cases alluding to the appreciation of unconventional moral values. Trolling often harasses and targets specific persons or institutions, rather than ideas and perceptions, thereby strengthening established (hardened) views, while disinformation is a more subtle activity to persuade or dissuade audiences, create confusion and sow discord.

The themes in the trolling campaign targeting Macron were related to his elitist background as a banker, his alleged lenient stance on immigration,[413] his supposedly homosexual inclination and claims of his supposed role as a US agent who is financially supported by foreign powers such as Saudi Arabia.[414] These themes are difficult to align with the overall narrative of an anti-EU or anti-liberal order and are palpably nonsensical to most observers. Furthermore, they do not fit well within the frames for the campaign since these themes are not socially divisive in France. The trolling campaigns did not persuade audiences to change their view and were ill-attuned to the fluid and multi-candidate political landscape before the 2017 presidential elections.

The activities of the grooming campaign, though aiming to support all candidates with a pro-Russian, or anti-EU and anti-NATO inclination[415] were focussed on Le Pen, not least since she requested support from Moscow.[416] Le Pen met Putin in Moscow on 24 March 2017, and expressed her approval of the Russian annexation of Crimea, and her opposition to the subsequently imposed EU-sanctions. Earlier, in 2014, Le Pen's FN had received an €11 million loan, €9.4 million of which came from the First Czech-Russian Bank in Moscow, affiliated to the Kremlin.[417] However, the support for Le Pen lay largely outside cyberspace and could be classed as traditional 'political warfare'.[418]

[412] Yaoi is Japanese gay manga (graphic novels). See also: Jeangene Vilmer, "Lessons from the Macron Leaks." p. 77; Ryan Broderick, "Here's How Far-Right Trolls Are Spreading Hoaxes About French Presidential Candidate Emmanuel Macron," BuzzFeed News, 2017, https://www.buzzfeednews.com/article/ryanhatesthis/heres-how-far-right-trolls-are-spreading-hoaxes-about#.ymk7oozeG.

[413] Ben Nimmo and Camille Francois, "# TrollTracker: Glimpse Into a French Operation," *DFRLab*, November 28, 2018.

[414] Jeangene Vilmer, "Lessons from the Macron Leaks." p. 76; EU vs Disinfo, "Tackling Disinformation à La Française," 2019, https://euvsdisinfo.eu/tackling-disinformation-a-la-francaise/.

[415] These include the far left Mélenchon, and the centre right Fillon, see also: Nougayrède, "Spectre of Russian Influence Looms Large over French Election Officials Are on Alert for Campaign Meddling."

[416] United States Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election-Volume 5: Counterintelligence Threats and Vulnerabilities." pp. 401-402; Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 24.

[417] Jeangene Vilmer, "Lessons from the Macron Leaks." p. 78; Limonier and Petiniaud, "Mapping Cyberspace: The Example of Russian Informational Actions in France." p. 50; Gabriel Gatehouse, "Marine Le Pen: Who's Funding France's Far Right?," BBC News, 2017, https://www.bbc.com/news/world-europe-39478066.

[418] As meant in the RAND study, Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*.

4.4.5. Exploiting social media

Cyberspace was exploited to amplify the cyber-related activities,[419] also by employing bots.[420] Social media account, including Twitter, with links to Wikileaks repeated messages especially related to the hashtag #MacronLeaks. In the run-up to the elections, US alt-right accounts and bots 'had previously attacked the Democratic Party to help Donald Trump in the 2016 US Presidential Elections'.[421] Apart from magnifying content via Twitter, RF news outlets RT and Sputnik facilitated the repetition of fabricated news items or shared and magnified trolling campaigns.[422]

Amplifying and magnifying the content by increasing the reach and intensity of the repetitions was conducted by RF but also by US alt-right and French far-right entities. These two groups of agents and individuals might have been aware of each other's activities, and their interests – the smearing of, and spreading rumours about, candidate Macron – coincided, but whether it was a coordinated effort is questionable.[423]
Amplifying the frames used in the cyber-related activities could have been less effective due to misinterpretations on the part of the RF or US alt-right agents. Misinterpretation might have occurred due to flawed translations from English to French, or from a misinterpretation of French electoral rules and legislation.[424]

Repeating messages was hampered since French mainstream media are inclined to be restrictive in broadcasting political advertisement. Ads that are aired are free, equal in time and in number for each political party.[425] Furthermore, where candidate Trump tweeted 4,994 times between the announcement of his candidacy and election day, in France traditional media still dominated the political landscape and discourse,[426] although newspapers and television debates had lost terrain due to the emergence of social media,

However, the effect of social media was not void. During the campaign Le Pen used a frame which linked the influx of migrants to the economic problems, unemployment and the

[419] Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 3 & annexes.

[420] Howard et al., "Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter?" Pp. 4-5; Alexander Frame and Gilles Brachotte, "Engineering Victory and Defeat : The Role of Social Bots on Twitter during the French PresidentialElections," in *Comparing Two Outsiders' 2016-17 Wins: Trump & Macron's Campaigns*, 2018.

[421] Martin and Shapiro, "Trends in Online Foreign Influence Efforts." p. 32; Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 3.

[422] Disinfo, "Tackling Disinformation à La Française."

[423] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." p. 23; Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 3.

[424] Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 3.

[425] Hansen and Lim, "Doxing Democracy: Influencing Elections via Cyber Voter Interference." p. 164.

[426] Maarek and Mercier, *La Présidentielle Chamboule-Tout. La Communication Politique Au Prisme Du « dégagisme »*. Part 3, Chapter on 'Retour sur la couverture télévisée de la champagne'.

declining welfare state of France in an effort to combine socially divisive topics with the stereotyping-, confirmation- and anchoring heuristics regarding people from abroad. Despite the efforts of critical journalists to fact-check and counter Le Pen's framing, paradoxically there was increased attention for the topic.[427] Fact-checking improves the factual knowledge of voters which alluded to the more rational aspects of a frame, but will not take away the subconscious cognitive and social heuristics that are raised in the frame.[428]

Though the potency of social media was present during the campaign, and the methods used were similar to the US presidential election campaign, the exploitation of social media to magnify and amplify cyber-related activities was less effective due to flawed framing and the lack of strong domestic influence operations.

4.4.6. Generating effects

'EU vs Disinfo' argued that the RF strategy was 'to spread many false narratives via different tools and methods – and then wait for them to be amplified, first with the help of 'hacktivists' and the 'cyber underground', then social media, and finally the traditional media.'[429]

Nevertheless, the impact of the influence operation by the RF, supported by US and French alt-right communities[430] during the 2017 presidential elections appeared to be marginal and the influence operation failed, according to Vilmer.[431] This does not mean that France is immune to foreign election interference. Knowingly, France adopted new legislation concerning the fight against information manipulation in December 2018.[432] It is likely that foreign agents learn from earlier mishaps, as, for example, RT and Sputnik are in the process of closing the (French) language gap.[433]

The question why the influence operations failed to achieve effects is challenging since there is no official document stating the RF purpose, and RF remains silent on the matter.[434] Moreover, there has not been a national inquiry similar to the UK House of Commons

[427] Oscar Barrera et al., "Fake News and Fact Checking: Getting the Facts Straight May Not Be Enough to Change Minds," 2017. pp. 3-4. Barrera et al., "Facts, Alternative Facts, and Fact Checking in Times of Post-Truth Politics." pp. 15-18.

[428] Peter Pomerantsev, "To Unreality — and Beyond," *Journal of Design and Science*, no. 6 (2019). p. 11.

[429] Which did happen, if only to debunk the topic. See: Nathalie Raulin, "Macron Gay? L'intéressé Se Marre," *Liberation*, February 7, 2017.

[430] Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election."

[431] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem." pp. 26-40.

[432] Assemblée nationale, "Loi Relative a La Lutte Contre La Manipulation de l'Information (1) (No 2018-1202)" (2018).; Richard Rogers and Sabine Niederer, eds., *The Politics of Social Media Manipulation* (Digital Methods Initiative, University of Amsterdam, 2019). p. 41.

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

[434] Thomas Brewster, "Did Russia Hack Macron? The Evidence Is Far From Conclusive," *Forbes*, May 2017.

'Disinformation and 'fake news''- inquiry or the US 'Report on the Investigation into Russian Interference in the 2016 Presidential Election (the Mueller Report).

Scholars, including Jeangene Vilmer and Ferrara, argue that the Russian attempt had limited success in affecting the outcome of the French presidential election.[435] The attempt to influence the election was hampered from the start due to insufficient preparation and RF operatives' lack of linguistic and cultural skills tailored to the French political landscape.[436] The hack required to gain authentic material on Macron did not result in the collection of sensitive or confidential data. Neither could the RF rely or piggyback on a strong domestic influence campaign by e.g. Le Pen or Melenchon. As a result, the operationalisation of the narrative in frames was less than perfect; consequently the cyber-related activities including the leaking of information and the supporting disinformation campaign did not catch on. This might have resulted in a shift to smearing, mockery and personal attacks, in particular on candidate Macron. This trolling campaign was strengthened by the contribution of pro-Russian US alt-right activists and French far-right activists favouring Le Pen over other candidates and at the same time, defaming Macron. All in all, the intense trolling campaign did not address genuine French political topics: the economic gloom, terrorism and the role of Islam, the role of the EU and the disillusionment with the existing political establishment. Due to the flawed frame which lacked current socially divisive topics nor addressed genuine cognitive and social heuristics of the audiences, the content of the cyber-related activities was not picked up by the dominant traditional French media.

4.4.7. Concluding remarks

It can be concluded that the influence operation during the French presidential elections was a piecemeal and not a fully-fletched RF influence operation. However, due to the lack of an on-going domestic influence operation in France and a deficient understanding of French societal topics and preferences of the populations, the framing was flawed. Though the intrusion on the Macron campaign team was successful, the content of the documents stolen during the hard-cyber hack, was futile. The subsequent cyber-related activities have been described as 'amateurish, chaotic, disorganized, and has little substance to it'.[437] The disinformation campaign trying to persuade the French audience ended up as a trolling campaign supported by French and foreign agents with alt-right affiliations,[438] hence it was not credible nor did it address genuine divisive topics for the French population.

[435] Jeangene Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."; Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election.".

[436] Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." P. 15 (discussion and conclusion)

[437] Soesanto, "The Macron Leak That Wasn't." p. 4.

[438] Ferrara, "Disinformation and Social Bot Operations in the Run Up To the 2017 French Presidential Election." p. 1.

Section 4.5.: Key Findings

On résiste à l'invasion des armées;
On ne résiste pas à l'invasion des idées.[439]

This chapter does not provide an assessment of whether influence operations have changed the results of the vote in these elections,[440] nor what the impact of social media was on the political discourse. After all, social media did not create the societal and political issues in the UK, France and US, they articulated them.

This chapter has given a description related to the sub question: "*How were the influence activities executed during the 2016 UK EU referendum, the 2016 US presidential election, the 2017 French presidential election?*"

Influence operations aim to affect the cognitive dimension of the targeted audiences, and in the cases under discussion these are in essence remote soft-cyber operations that deploy cyber-related activities initially from outside the target State. In general, influence operations in cyberspace deviate from traditional operations in the sense that they are not linear. Given the cases,

The influence operations all followed a similar sequence of preparing, executing and exploiting the cyber-related influence activities, though not all influence operations executed all these phases and it cannot be taken for granted that influence operations are activities which are prepared, executed and exploited by one State (or a coalition of States). Furthermore, during the phases of an influence operation, a State can be supported by other actors, State or non-State, foreign or domestic, as in the French case where US alt-right communities targeted Macron and supported Le Pen. Cooperation is thereby rather based on an ad-hoc combination of interests than on a coordinated plan.

A State can choose to employ a full influence operation, such as during the US presidential election, in which preparation, execution and exploitation are State-led, or it can choose a piecemeal approach by which the State engages during phases or subphases supporting and

[439] Victor Hugo

[440] An answer which is difficult to give, see: Andrew M. Guess, Brendan Nyhan, and Jason Reifler, "Exposure to Untrustworthy Websites in the 2016 US Election," *Nature Human Behaviour*, 2020. p. 18. Christopher A. Bail et al., "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences of the United States of America* 117, no. 1 (2020): 243–50. p. 243.

enhancing on-going existing domestic influence operations, as happened during the UK EU referendum and the 2017 French presidential election.

Though three different phases can be distinguished during influence operations, they do not have a chronological pattern. During the execution of elements of the influence operation new data can be harvested or hacked to prepare another strand in the operation. Likewise, the execution of a trolling campaign can run parallel to the exploitation of an earlier disinformation campaign.

Though influence operations are inherently soft-cyber operations, hard-cyber activities i.e. hacking into foreign ICT systems to steal, collect or copy data, can be used to support the preparation of the influence operation. During the 2016 US presidential election and, to a smaller extent during, the 2017 French presidential election, both hard- and soft-cyber activities were employed. The hard-cyber activities were mainly used in the preparation phase as supportive activities of the influence operations.

As set out in Chapter 2, the description of the cases, follow a three-phased pattern related to the preparation, execution and exploitation.

4.5.1. The preparation

The RF did not create specific strategic narratives for any of the cases. Existing informational instruments of power related to anti-EU (in the UK and French cases), anti-NATO (in the French case) or anti-liberal democracy (in the US and French cases) narratives were used. This was done with the purpose of creating strategic confusion, or of 'sowing doubt about democracy, the leadership, and one's ability to exert any influence on the democratic system.'[441]

Framing the strategic narratives is a crucial part of the preparation phase for influence operations. During framing, the more conscious socially divisive topics (economic decline, race, unemployment, police violence) are coupled to ingrained preferences of specific audiences that need to be invoked to influence the targeted audiences.

Framing worked well during the UK case, not least since the frames were generated by domestic actors that had profound knowledge of the English language and culture and social grievances in Britain. The Leave camp generated strong frames, including 'take back control'. The aim of the Leave-camp coalesced with the RF anti- EU narrative.

[441] Disinfo, "Tackling Disinformation à La Française."

The US Case was different in reach and extent. The RF executed an independent influence operation that had been building up since 2014. The RF influence activities were not limited to remote operations from abroad. RF agents were temporary residents and worked from the US. The frames the RF made during the influence operation in the US Case revolved around weakening the campaign of Hillary Clinton, while supporting her opponents, which in the end meant supporting the presidential campaign of Donald Trump. The RF frames were well adjusted to current socially divisive topics such as racial issues and police violence, but moreover they invoked the right heuristics and preferences of the audiences, anchoring Clinton to the image of dubious moral judgement and covert political deals.[442] The long-term preparation may have been conducive to the effort, together with thorough research, the use of auxiliary actors (Cambridge Analytica), enhanced by lessons learnt in other areas.[443]

The French framing was flawed due to the RF lack of cultural knowledge and command of the French language, and perhaps to the absence of a consistent domestic influence operation as witnessed in the UK. Furthermore, there was no obvious political divide similar to the US case. In the US the division in party ideology was reinforced anti-establishment sentiments. It also differed from the UK referendum that witnessed an overarching campaign theme: in-or-out of the EU.

Hard-cyber operations were used to support the preparation of the influence operations in the US and French Case. During the US Case the Clinton campaign team, the DNC and the DCCC were hacked, so the RF agents were able to obtain sensitive and confidential data. The yield from the hack on the Macron campaign team was poor and therefore difficult to exploit. In the UK Case, no hack was recorded (or made public). In that case, the data were collected by domestic parties, especially related to the Leave-camp, using the services of Cambridge Analytica and AIQ.

4.5.2. The execution

In the UK Case, the RF influence operations were in support of ongoing domestic influence campaigns and particular in favour of the UK Leave camp, thereby defaming Remain-politicians and bolstering the Brexiteers, most prominently UKIP's leader Farage.

The RF main effort during the US presidential election was the controlled leaking of sensitive information undermining the integrity of candidate Clinton. The activities were supported by disinformation campaigns addressing topics ranging from Islam, Religious beliefs, Black Matters, police violence, to the independence of Texas. In the run-up to the US election

[442] Tom Uren, Elise Thomas, and Jacob Wallis, "Tweeting through the Great Firewall," no. 25 (2019). p. 5.

[443] Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." p. 236.

numerous RF agents masqueraded as US nationals, writing in English from US-based Twitter or Facebook accounts. Often these deceitful accounts were appreciated as genuine.

The French presidential election was characterised by a leaking and trolling campaign, supported by smaller disinformation campaigns, rendering political backup to the Le Pen campaign. The leaking of information, however, proved ineffective, partially due to the lack of any damaging data obtained from the Macron campaign team hack.[444] Attempts to doctor the leaked documents make them inauthentic and therefore ineffective. The lack of sensitive data, may have been the reason why the influence operation resulted in an exaggerated, even preposterous, trolling campaign that did not catch on since it did not address genuine socially divisive topics, including the state of the economy, terrorism or the disillusion with the then political establishment.

4.5.3. The exploitation

Exploiting social media was well-developed during RF influence operations. The RF was able to generate numerous bots and human agents to amplify and magnify content. Moreover, the RF had the ability to synchronise public and private media outlets, not least since it controlled many outlets and media companies including RT and Sputnik.

In the UK EU referendum case, exploiting content on social media was the core activity. The RF magnified and repeated the Leave camp frames via the elaborate use and exploitation of social media.

The exploitation of social media by RF was also extensive in the US Case, using a multitude of social media platforms, YouTube and WikiLeaks. It can even be argued that the RF influence operations increased the polarisation between opposing groups (particularly between the Democrats and the Republicans) by extensively amplifying messages to ideologically like-minded groups,[445] thereby undermining public discourse which is the key attribute of the liberal democracy.

In the French Case, exploiting the cyber-related activities via social media was most likely dominated by US alt-right communities and French far-right entities advocating Le Pen, rather than by the RF.

[444] Toucas, “The Macron Leaks : The Defeat of Informational Warfare.” p. 3.

[445] Bail et al., “Assessing the Russian Internet Research Agency’s Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017.” p. 243.