ANALYSING RUSSIAN CYBER-WARFARE AND LEGAL FRAMEWORKS IN THE CONTEXT OF UNITED STATES ELECTIONS 2016

Seerat Fatima and Asfa Azam[*]

Abstract

This paper explores the evolving nature of warfare in the 21st century and its impact on international law. While violence has always been a part of the anarchic international system, technological advancements have continually reshaped warfare. The integration of Information and Communication Technologies (ICTs) has introduced digital infrastructure, allowing states to engage in unconventional warfare to protect their national interests. The alleged Russian interference in the 2016 U.S. elections exemplifies this new form of conflict, challenging the traditional frameworks of international law. This incident has raised concerns about the ability of existing legal structures to address the emerging threats posed by cyber and information warfare. The study argues that to effectively regulate state behaviour and respond to contemporary challenges; international law must evolve alongside technological advancements or risk becoming inadequate in the face of modern geopolitical struggles.

Keywords: Cyber-Warfare, Information Warfare, Electoral Interference, International Law, Budapest Convention, Tallinn Manual 2.0.

Introduction

In the face of the 21st century, the rapid evolution of information communication technologies has extensively reshaped the landscape of the global system. It has set forth the stimulus of contemporary challenges for the international system of states, which has disrupted the landscape of national and international conflicts over a short span of time. Meanwhile, the case study of the United States elections in 2016 foreseeably affirmed the erosion of the traditional character of warfare while putting international law at the odds of being ineffective.

[*]Seerat Fatima is a graduate from National Defence University, Islamabad. She has completed a dissertation as part of her academic journey. Asfa Azam is a graduate of Strategic Studies from National Defence University, Islamabad.

The United States electoral process in 2016 remained at the gamble of transnational political warfare induced by Russian statecraft through alleged cyber and information warfare. This conduct deliberately introduced a distinct form of fourth-generation warfare at foreplay. Russia was allegedly successful in enabling the political tool of disinformation campaigns as part of information warfare and the technological course of cyber warfare to sow the seeds of political chaos without kinetic confrontation against the United States. It was consistently directed by the strategy of clandestine diplomacy paved by the political leadership of Russia to synchronize the course of action in an organized manner. At the disposal of political interference, it yielded tactical disruption of opinionated narratives within the political sanctity of the United States and remained consequential in swindling the elections. Meanwhile, International law is reflected as a premature entity to assess the case because the interpretation of its articles vaguely qualifies cyber and information warfare as the use of force against a state or outlines as direct involvement. For this reason, Russia, to date, has the liberty to escape the allegations assuming the limitations of international law. To be precise, the Russian transnational political camouflage stretched across the governance infrastructure of the United States challenges the position of international law in terms of preserving the sovereignty rights of states. It is not every now and then that a state like the United States faces the ground-breaking influence of externally plotted factors over its democratic electoral processes while Russia flees without any legal consequences. For the matter of concern in the aforementioned scenario, this research article aims at thorough corroborative discourse within the literature to understand that if manipulating the results of hegemonic power can be a possible reality without any judicial proceedings, then the prevalent evil is expected to spread across the international system of states and the standing of international law as guardian of international peace shall be at the stake**.**

Analytical Overview of United States Elections 2016

The presidential elections of the United States in 2016 were unique because of several unprecedented events that shaped its national political landscape for years to come. These events are the underlying factors that led to the final outcome of the U.S. Election 2016. As it is not out of the blue that Donald Trump treaded the success story of becoming the President of the United States, it is pertinent to bring forward these factors.

During the Presidential Elections of 2016, the Democratic and Republican divide expressed a fierce political battle between competing nominees. Moreover, it is considered to be one of the most polarising Elections in the history of the United States.[1] Hillary Clinton, being the representative of the Democratic Party, and Donald Trump, being the representative of the Republican Party, expressed their reverent arguments over the State's key issues.[2] Hillary Clinton showed up with empathy and ideal conditionality, while Donald Trump was impeccably in opposition to her contender's viewpoint.[3] He showed up as a populist figure who sided with the working class against the corrupt elites of the nation.[4] He used to be in the spotlight of media coverage for his controversial but equally popular ideas.[5] Donald Trump and the extravagant influence of their populist drive flared up an immense uproar among voters against the stagnant issues of immigration, terrorism, job security and the American approach to internationalism.[6] He came up with the simple but popular slogan of "Making America Great Again" to reflect the commitment of his vision with the state.[7] Moreover, it was carefully crafted to remind the American nation of Islamic terrorism, which previously was responsible for the unprecedented attack of 9/11, in order to create a divine battle against the evil of terrorism.[8] He facilitated the narrative of Islamophobia in the United States by owning a Muslim ban in the United States.[9] This envisaged nationalism was an appealing manifesto for the general public of the U.S.

The political campaign of Donald Trump was very cautious in targeting the sentiments of workers in rust belt cities who were resentful of the prevalence of declining heavy industries and employment.[10] The group of people lies on the fringes of metropolitan life and are highly unsatisfied with the term of Barack Obama.[11] Trump was becoming popular among abandoned citizens of the United States, and this resulted in his campaign with the unwavering support of the Rust Belt cities of the United States.[12] On the other hand, the Democratic Party was losing favorable grounds in these cities against the Republican Party and ultimately met with a significant transformation of the political landscape.[13] However, these aforementioned political leverages were not enough to manifest Donald Trump as the most eligible candidate for the U.S. public in terms of presidency. Rather, there were other externally derived social derivatives involved, which ensured a successful attempt to lure voters to choose Trump as president of the United States, and it did remain successful.

These external factors of influence, which were successful in by-passing national borders, include the role of Cambridge Analytica for substantiating the tactical drive of social media in favour of Donald Trump while targeting the image of Hillary Clinton and allegedly intentional database hacking by Russian leadership in order to influence the national electoral process of United States.[14] Meanwhile, Russian involvement is still argued because of the consistent denial by Russian Premier Vladimir Putin was communicated several times, and this brings the raising concerns for a liberal democracy to get exploited without the enemy being convicted.

Russian Propaganda of Cyber Operations against US Elections 2016

Russia is allegedly considered to have shown covert participation in the United States Elections 2016.[15] Even with its denial account, Russia is evidently accused of having interfered in the US elections to influence the presidential election.[16] Moreover, it was evidently discovered from the Kremlin secret documents that Russia was secretly but actively executing a plan to support the US Republic candidate Donald Trump during the United States elections 2016.[17] Russian intent was an imminent approach to place Donald Trump as the president of the United States. For some reason, Russian Premier Vladimir Putin considered Trump as one of the right people to favour Russia on foreign policy grounds. It was evident after Trump was elected as the president of the United States during a conference when Putin's denial of interference in elections was considered truer than that of the US Intelligence report.[18] Russian hacking operations, cyber warfare operations and disinformation campaigns are a combination of political, cyber and military operations which were allegedly directed against the United States Elections 2016.[19] It is an integral part of their activities in the world, and the most interesting component of that is called kompromat, which means to compromise you through some demeaning degrading or information that is embarrassing in order to either knock you off guard or throw you into chaos for their advantages.[20] That was exactly what the Russians did in the United States Elections 2016.

The purpose was not only to create chaos at the Democratic National Convention (DNC). It was designed to create chaos in the United States.[21] Anything that would create destabilization within the liberal Western democracy works for Russia.[22] Russians were carrying out a massive cyber warfare operation against the United States, which is why it was traced

precisely with the analysis reports of the CIA.[23] This was not just Wiki leaks releasing information that was hacked; this was a national security emergency. That the United States itself was under attack by a hostile government through the machinations of its hostile intelligence agency, what used to be known as bullet collusions, a former organisation the KGB, now the FSB.[24] For ten months, Russians were using cyber hacking tools, and they virtually stayed inside the service of the Democratic National Committee across the encrypted data space.[25] Meanwhile, they were stealing every document available and were transferred to each other via real-time chats that were monitored. [26] Later on, it was revealed that they were monitoring every chat between DNC and later revealed that the DCCC, the democratic congressional campaign committee, was also hacked by the Russian intelligence force as well and there was a company called Crowd Strike that was brought into the Democratic National Committee at the time of the hacking.[27] The CEO of Crowd Strike said we were sitting there on computers, everybody watching the files get transferred one at a time and then watching them erase their footprints, and these servers were in Russia in servers related to the FSB.[28] Then, an entity popped up called Guccifer 2.0, a Russian hacker who had all the information from the DNC and wanted to leak it to the news media.[29] This was just a front entity being used by the FSB to leak this information as it became known information. Meanwhile, it started to leak out a little bit later in late July that Julian Assange claimed that he had all of the DNC emails now it is possible that some private hacking group got into those emails and could have done that, but it is impossible that they would have left the fingerprints of Russian intelligence material going back to KGB or FSB.[30] The rationale of the aforementioned operation was to extract sensitive information from the encrypted sources of the national agency of the United States in order to proceed with the cumulative plot ahead. Since the disguise was to maintain these activities, Russian leadership remained consistent in denying it on international platforms and carried on eliminating all the threads of evidence from its side.

Modus Operandi of Russian Cyber and Information Warfare in Elections

In the case of Russian Hybrid interference in the United States Elections 2016, the dawn of code war was indicated as a potential intangible threat to the state after this stage. The misuse of cyberspace was not new, but its

ability to threaten the autonomy and sovereignty of a state at the leadership level by breaching domestic digital privacy was something big.[31] The use of psychographics merely for the purpose of disinforming the masses was something new.[32] Making unpredictable realities of human perceptions predictable at such a fast pace merely by imposing perceptions from outside without firing a bullet was a bombshell. So, it's like a boomerang. You send your data out; it gets analysed, and it comes back to you as targeted messaging to change your behaviour.[33] The intangible nature of espionage transcending the concrete borders was a mere question mark over preserving sovereignty. It highlighted the mere crisis of preservation of digital privacy rights. Moreover, Christopher Wylie, former data scientist of Cambridge Analytica, said, "It is incorrect to call Cambridge Analytica a pure sort of data science company or an algorithm company; in effect, it is a full-service propaganda machine".[34] People don't want to admit that propaganda works because to admit means confronting their own susceptibilities, horrific lack of privacy and hopeless dependency on tech platforms, which ultimately is ruining the democracies on various attack points.[35]

In this technologically advanced era, data companies have acquired the most valuable asset on earth, which is information data. The morphology of information data is flexible for the user, and data companies are experts in changing the forms.[36] Cambridge Analytica in the US 2016 Elections, even if notoriously, showed how predictable it can be with data in different forms. It executed a psychological operation named Project Alamo on 50 million people, which initially identified the right audience to target, disrupted existing perception and then incepted altered virtual reality to inform the audience to meddle in the votes for the victory of its client.[37] The linkages of the client, the Donald Trump, lead to reveal alleged involvement of Putin's administration through cyber penetration under safe heavens of Cambridge Analytica in the United Kingdom. This back-door diplomacy of Moscow to make Washington far more predictable for the course of its benefit in the international system without engaging in real-time war rather than virtual raised concerns over invisible doors of cyber which has provided potential arms to target persuasion of state.[38]

Psychological operations in military affairs have long been volatile and acceptable as well till it was for the preservation of the National Security of a state and limited to combatants, but since it has penetrated the political

affairs of a state across borders through sophisticated use of cyberspace has posed real-time threat to institutions of democracy.[39] It is similar to bringing battle games of combatants at battlegrounds to the social ailment of inter-connectedness by targeting the autonomy of a nation without letting the people know about it. Similarly, the level of impact that psychological operations had on political campaigns, especially the way it did in the US Elections 2016, has raised critical apprehensions over the likelihood of state failure to acknowledge the legitimacy of democracy among people.

The Threat to democracy of a democratic state is equivalent to a National Security Threat no matter how silent, invisible and complicated the origin is. This threat is a danger to states from data companies meddling in political matters. The extent of impact data companies have achieved through the sophisticated technologies of Artificial Intelligence and data mining in the field of psychological operations is worth concerning for state institutions because it has threatened the state's monopoly of autonomy. US Elections 2016, with the complicated web of networking and data profiling, affirmed the need for social cyber security as a guardian of emerging sciences.

Psychographics have been potentially significant perpetrators in revolutionizing the modes of Digital political campaigns while being the manipulator of Cambridge Analytica in US Elections 2016 through weaponization of cyberspace with privacy breaches and disinformation.[40] It acquires the potency of inflicting serious injuries to the realistic world advocacies by constructing virtual alterations, the only reliable reality for consumers. [41] US elections in 2016 were the manifestation of the aforementioned virtual scam, which was morally subjected to criticism.[42] It provides us with the perfect model to identify the dualistic nature of psychographics along with AI as a marketing and political tool in quantifying the perceptions of the majority, then molding it for a notorious plot with the art of visually altered reality accordingly.[43] Subsequently, it has the potential to manipulate the democracy of a state by altering the perceptions of citizens, compromising their rights of autonomy.[44] It is an emerging concern for nation-states regarding their sovereignty where narrative deciphers the sole purpose of keeping national cause intact, and the moment it is at the target of malicious use of psychographics, then stakes get beyond.[45] This enacts security concerns for the democracies of states, which are part of ever-evolving cyber reality, and US Elections 2016 confirmed

that psychographics can potentially overcome the cognitive ability to harm non-tangible assets of a state with the amalgam of AI and cyber disinformation.[46] Brittany Kaiser declared psychographics a weapon-grade out-source of cyber technology in order to put up the realization of real-time challenges for statecrafts regarding the potential psychological warfare tool.[47] The purpose of this extent of politicizing involves serious addressing of the issue, especially when the threat poses serious implications for the National Security of states as it did during the US Elections 2016.

Interpretation by International Law

The preamble of the United Nations, at its core, deals with the enforcement role as global sheriff, reflecting the daunting authority of International Law against the anarchic system of states. It counts on keeping the harmony of political standing among member states against the possibility of war and its looming consequences. While it has successfully denounced the all-out war so far but the recent introduction of information communication technology raises questions over its pretext of being relevant to contemporary issues. This is evident in the case mentioned above study of Russia's alleged interference in the United States Elections 2016, which presents an unusual form in terms of the exclusive genre of warfare.

The democratic process of the 2016 U.S. elections was influenced by altering the behaviours of the voters through externally plotted cyber-oriented measures.[48] This is pretty strange from the context of International Law in its literal interpretation of article 2 (4) and article 2 (7) of the United Nations Charter. It is because the objective interpretation of provisions exposes weak judicial and legal argument by indistinctly defining the definition of 'force'. The consequential evidence of cyber-driven intrusive crimes across jurisdiction may qualify the accusation of rupturing the sovereignty of the United States as stated by Article 2(7), but they fail to meet the criteria of Article 2(4) because these activities do not cause physical disruption, collateral damages or loss of life.

Apart from the political ramifications, digital infrastructures pose a threat to the fundamental right of self-determination.[49] Since the unusual activity was conducted across all accessible information communication platforms, the opinionated narratives were crowded with the simulated coverage of new reality on social media.[50] It allowed the general masses, including the voters,

to make decisions based on the altered information surrounding them.[51] It led to the exploitation of the liberal democracy of the United States without any real-time confrontation with Russia. It takes the discourse to identify the role of international law. The digital sovereignty of the United States teetered on the brink of collapse due to significant manipulation provoked by externally instigated operation orchestrated by Russian leadership.[52]

It was revealed that cyber-attacks like these, which may not meet the requirements of traditional armed attacks, are not entirely governed by the laws of armed conflict. Instead, frameworks such as the International Law of Countermeasures or domestic laws regulate them. Given the universal nature of cyber-attacks, a coordinated international solution is required, starting with the development of common definitions of terms like 'cyber-attack' and 'cyberwarfare.' The 'Paris Call' and support from international bodies like the European Union or NATO highlight the need for these legal frameworks.

The situation led to the prevalence of a trust deficit between the political authority of the state and insecure citizens within the United States who were facing the challenges of a compromised democracy.[53] In this regard, the national security of the U.S faced several psychologically and perceptually induced threats directly challenging its democratic value system, which has been ethically compromised. These actions contributed to the accumulation of political factors responsible for instability and social disintegration, posing a significant threat to the domestic harmony of the democratic state in the face of external cyber threats.[54] Cyber-attacks like these demonstrate the necessity to better understand the legal landscape of cyber conflict, as future conflicts are likely to include cyber components. In this way low-end technological efficacy provided Russia, as an external actor, with the liberty to induce crisis situation for the United States without kinetic confrontation.

Specifically, Article 2(4) of the UN Charter prohibits the use of force against the territorial integrity or political independence of any state.[55] However, cyber operations like those allegedly carried out by Russia data breaches and disinformation of data breaches do not result in physical damage, which is traditionally defined as armed conflict under jus ad bellum.[56] While these actions could be interpreted as violating article 2(7), which is about protecting state sovereignty from external or foreign intervention, such actions fall into a legal grey area as these are not properly addressed by International Law. Moreover, International Law does not clearly define

cyber-attacks as an 'act of war' either. Such situations of ambiguity cause challenges of attribution and also how the states against which the attack is carried perceive and react after it. Furthermore, the cyber-operations allegedly committed by Russia do not meet the criteria for an armed attack, which is the threshold required to invoke self-defence under Article 51 of the UN Charter.

In addition to this, international legal bodies such as the International Court of Justice (ICJ) have not fully developed legal jurisprudence for addressing non-kinetic warfare like cyber-warfare.[57] However, cyber operations can root significant disruptions to a state's democratic processes, as seen in the 2016 U.S. election. The absence of legal clarity or clear definitions and explicit prohibitions makes it difficult to hold the responsible state accountable for any such actions.[58]

Tallinn Manual 2.0 And the Budapest Convention are vital in the context of cyber warfare. They provide essential guidelines where international law has not adequately addressed the gaps related to cyber-attacks.[59] Tallinn Manual 2.0 was also designed for the actions that fall short of the use of force, particularly relevant in cases like the 2016 U.S. elections, addressing the key issues involved in the cyber realm such as sovereignty, non-intervention and prohibition on the use of force.[60] However, the manual remains limited in dealing with complexities involved in non-kinetic warfare like disinformation campaigns, which were a major feature of alleged Russian involvement in the 2016 U.S. elections and manipulation of the electoral processes.

Another relevant legal framework is the Budapest Convention on Cybercrime that addresses cybercrime by harmonizing national laws, improving investigative techniques and cooperation among states.[61] In the case mentioned above, it criminalizes the cyber activities allegedly carried out by Russian operatives, such as hacking the DNC and dissemination of sensitive information. However, the state-sponsored, politically motivated cyber-operations are not directly addressed, limiting its applicability.[62] All in all, Tallinn Manual and the Budapest Convention play complementary roles and emphasize the importance of international cooperation in dealing with the complex nature of cyberspace.

Proposed Reforms in International Law to Address Electoral Interference

In this research article, the central argument remained discussed around the conception that Russian interference in the elections of the United States in 2016 has contributed to the prevalence of international security threats. Meanwhile, international law failed to criminalize it by placing it nowhere around the threshold of threat perception as per its constituency. This particular situation has forged serious apprehensions towards the sustenance of international peace. Because international law reflects lucid standing for its integral role in avoiding the contemporary threats of cyber information war crimes. Rather, it has been articulated over containing confrontational crimes among sovereign states, which is redundant in the contemporary age of revolutionary warfare practices. The international security lag requires inclusivity within provisions of international law for cyber operations, transnational data breaches and digital volatility. For this very purpose, following are proposed reforms for international law in order to contain the cycle of prevalent chaos across the theatre if international system:

- Criminalize state-sponsored data theft, transnational micro-targeting of national populace, and cyber security crimes, which are supported by binding propositions of an enforcement framework. Furthermore, it is proposed to predominately channelize update-ness and inclusivity for the upright stature of International Law.

- Establish an international electoral security body based on the revolutionary science of cyber forensics and intelligence sharing with the mutual cooperation of member states. It is essential to monitor and track political and cyber-laden irregularities of foreign origin that disrupt the electoral process.

- Instill coercive measures of economic and diplomatic isolation for the convicted state. Since the flow of transnational transactions and assets is the reality of the global trade structure, economic sanctions of transnational assets and referral to the International Criminal Court (ICC) are effective mechanisms to concede the spirit of exploitation. Meanwhile, a middle ground for political mediation and dispute resolution should be available as peaceful alternatives against the escalation of conflict.

- Format the joint cyber task force as an authoritative agency under the joint command of the United Nations Security Council and International Electoral Security Body to contain the transnational threats that have been discussed above.

- Address and amend the operative provisions under the principle of neutrality. Cyberspace is proposed to be included among the equally plausible mediums of war crimes. To be more elaborative, the illicit practices of cyber hacking and data breaches should be considered parallel to extra-judicial crimes by the sovereign authority of the state.

Conclusion

It is not to deny that the nature of violence is indigenous to mankind, and confrontational struggle has existed in the anarchic system of states, but the character of warfare was never static itself; rather, it remained imperative to the implications of technological advancements. For this reason, international law's strategic outlook is deemed dynamic. In the contemporary era of the 21st century, the widespread assimilation of information communication technologies disrupted the setting of the international system of states with the inception of digital infrastructure. It created the avenue for the unconventional scope of warfare among states to guard their respective national interests. Conclusively, the major reveal of Russian alleged interference in the United States Elections 2016 raised speculations to recognize the newly breaded scope of warfare, which happened to concede the relevance of International Law propositions in containing contemporary challenges of power politics.

References

[1] David Smith, "Where Donald Trump and Hillary Clinton stand on 2016's key issues," *The Guardian*, July 9, 2016, accessed December 25, 2023, https://www.google.com/amp/s/amp.theguardian.com/us-news/2016/jun/09/trump-clinton-economy-immigration-gun-control-environment
[2] Ibid.
[3] Ibid.
[4] Robert C. Rowland, "The Populist and Nationalist Roots of Trump's Rhetoric," *Rhetoric and Public Affairs* 22, no. 3 (Fall 2019): 343, accessed December 25, 2023, https://www.jstor.org/stable/10.14321/rhetpublaffa.22.3.0343
[5] Ibid, 345-372
[6] Jeremiah Morelock, "Donald Trump as Authoritarian Populist: A Frommian Analysis," in Critical Theory and Authoritarian Populism (University of Westminster Press, 2018), 73-75
[7] Ibid, 78-81
[8] Khaled A. Beydoun, "Donald Trump: The Islamophobia president," *Aljazeera*, November 9, 2016.
[9] Ibid.
[10] PARMAR, INDERJEET. "The Legitimacy Crisis of the U.S. Elite and the Rise of Donald Trump." *Insight Turkey* 19, no. 3 (Summer 2017): 9, accessed December 25, 2023, http://www.jstor.org/stable/26300527
[11] Ibid, 10-17.
[12] Min J. Lee, "Resetting red and blue in the Rust Belt," *CNN*, April 25, 2016.
[13] Richard C Longworth, "Disaffected rust belt voters embraced Trump. They had no other hope." *The Guardian*, November 21, 2016, accessed January 12, 2024, https://www.theguardian.com/commentisfree/2016/nov/21/disaffected-rust-belt-voters-embraced-donald-trump-midwestern-obama
[14] Reuben Steff, "The Audacity of Trump: How He Won and What We Missed." *New Zealand International Review* 42, no. 2 (March 2017): 2, accessed December 25, 2023, https://www.jstor.org/stable/48551982
[15] Robert S. Mueller, "The Report On The Investigation Into Russian Interference In The 2016 Presidential Election", Special Council of US Department of Justice, last modified 2019, accessed December 25, 2023, https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.justice.gov/archives/sco/file/1373816/download&ved=2ahUKEwjIjMuMyKqDAxXSi_0HHX6RAAcQFnoECBIQAQ&usg=AOvVaw3Lx_VrnoG0N_Gzxo6Hz4uM.
[16] Ibid.
[17] Luke Harding, Julian Borger, and Dan Sabbagh, "Kremlin papers appear to show Putin's plot to put Trump in White House," *The Guardian*, July 15, 2021
[18] Jeremy Diamond, "Trump sides with Putin over US intelligence," *CNN*, July 16, 2018
[19] Nance, *the plot to hack America*, 56-62
[20] Paweł Surowiec, "Post-Truth Soft Power: Changing Facets of Propaganda, Kompromat, and Democracy," Georgetown Journal of International Affairs 18, no. 3 (Fall 2017): 21, accessed December 25, 2023, doi:10.1353/gia.2017.0033.
[21] Ibid, 22-27
[22] Nance, *the plot to hack America*, 27-32
[23] Mueller, "*The Report On The Investigation Into Russian Interference In The 2016 Presidential Election".*
[24] Ibid.
[25] LAURA GALANTE, *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*, (Atlantic Council, 2022), accessed December 25, 2023, https://www.jstor.org/stable/resrep20718.
[26] Ibid.
[27] Kevin Collier and Donie O. Sullivan, "What is CrowdStrike and why is it part of the Trump whistleblower complaint?" *CNN Business*, September 26, 2019
[28] Nance, *The plot to hack America*, 88-92
[29] Ibid, 95-98
[30] Ibid, 101-107
[31] John P. Carlin and Garrett M. Graff, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (London: Hachette UK, 2018), 40-47

[32] Luke Stark, "Algorithmic psychometrics and the scalable subject," *Social Studies of Science* 48, no. 2 (April 2018): 204, accessed December 25, 2023, doi:10.1177/0306312718772094.
[33] Ibid, 207-228
[34] *The Great Hack*, directed by Jehane Noujaim, and Karim Amer. (2019; Utah, UT: Netflix, 2019), Film.
[35] Gordon Pennycook and David G. Rand, "Cognitive Reflection and the 2016 US Presidential Election," SSRN Electronic Journal 45, no. 2 (July 2018): 224, accessed December 25, 2023, doi:10.2139/ssrn.3110929.
[36] Ibid, 224-225
[37] Paul Lewis and Paul Hilder, "Leaked: Cambridge Analytica's blueprint for Trump victory," The Guardian, March 23, 2018, accessed December 25, 2023, https://www.google.com/amp/s/amp.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.
[38] Ibid.
[39] M. H. Errey, "Understanding and Assessing Information Influence and Foreign Interference," *Journal of Information Warfare* 18, no. 1 (Winter 2019): 1, https://www.jstor.org/stable/26894654.
[40] Ibid, 1-9
[41] Ibid, 7-19
[42] Nance, *the plot to hack America*, 65-71
[43] Shun Chiu, Kevin Kuan, C. Richard Huston, Hani I. Mesak, and T. Hillman Willis. "The Role of a Psychographic Approach in Segmenting Electorates' Voting Behavior and Party Identification." *Journal of Political Marketing* 9, no. 1 (February 2010): 34, accessed December 25, 2023, https://doi.org/10.1080/15377850903472521
[44] Nathaniel Persily, "The 2016 US Election: Can democracy survive the internet?" *Journal of democracy* 28, no. 2 (April 2017): 63, accessed December 25, 2023, https://www.journalofdemocracy.org/articles/the-2016-u-s-election-can-democracy-survive-the-internet/
[45] Jessica Dawson, "Microtargeting as Information Warfare," The Cyber Defense Review 6, no. 1 (Winter 2020): 63, accessed December 25, 2023, doi:10.31235/osf.io/5wzuq.
[46] Ibid, 63-67
[47] Lewis and Hilder, "Leaked: Cambridge Analytica's blueprint for Trump victory"
[48] Kellner, " Donald Trump, Globalization, and the Russia Connection in Election 2016," 140-147
[49] Dennis Broeders and Bibi V. Berg, *Governing Cyberspace: Behavior, Power and Diplomacy* (Lanham: Rowman & Littlefield Publishers, 2020), 50-57
[50] Jacob P. Matthews, "Defending Liberal Democracies Against Disinformation," *American Intelligence Journal*, 36, no. 2 (2019): 86, accessed January 2, 2024, https://www.jstor.org/stable/27066376
[51] Broeders and Berg, *Governing Cyberspace: Behavior, Power and Diplomacy*, 65-69
[52] Ibid, 73-79
[53] Francis Fukuyama, "American Political Decay or Renewal? The Meaning of the 2016 Election." *Council on Foreign Relations* 95, no. 4 (July/August 2016), 58. Accessed January 2, 2024. https://www.jstor.org/stable/43946933
[54] Ibid, 58-62
[55] Malcolm N. Shaw, *International Law* (Cambridge: Cambridge University Press, 2017), 982- 997.
[56] Ibid, 1048-1059
[57] Ohlin, Jens David,"Limits of the Sovereignty Framework." Chapter. In *Election Interference: International Law and the Future of Democracy*, 67–89. Cambridge: Cambridge University Press, 2020.
[58] Ibid, 69-85.
[59] Michael N. Schmitt, ed., "International Telecommunication Law." Chapter. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 284–300. Cambridge: Cambridge University Press, 2017
[60] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 13–15.
[61] Council of Europe, *Convention on Cybercrime*, Nov. 23, 2001, European Treaty Series No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[62] Ian Brown and Douwe Korff, "The Budapest Convention on Cybercrime: Ten Years on," *Computer Law & Security Review* 28, no. 5 (2012): 501–517.