ROLE OF SOCIAL MEDIA AND CYBER TECHNOLOGY IN THE RUSSIAN INTERFERENCE IN UNITED STATES' 2016 PRESIDENTIAL ELECTION

OBASI EXCEL TOOYA

PG/SSC1917785

A RESEARCH THESIS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE MASTER OF SCIENCE (M.Sc.) DEGREE IN POLITICAL SCIENCE (INTERNATIONAL RELATIONS) SUBMITTED TO THE DEPARTMENT OF POLITICAL SCIENCE, FACULTY OF ARTS AND SOCIAL SCIENCES, UNIVERSITY OF BENIN, BENIN CITY, EDO STATE. NIGERIA

SUPERVISOR

DR. AKPOMERA

JANUARY, 2023

CERTIFICATION

This thesis entitled, ROLE OF SOCIAL MEDIA AND CYBER TECHNOLOGY IN THE RUSSIAN INTERFERENCE IN UNITED STATES' 2016 PRESIDENTIAL ELECTION, prepared by TOOYA EXCEL OBASI, PG/SSC1917785, has been carefully read, supervised and approved as having satisfied the thesis conditions for the award of Master of Science (M.Sc.) Degree in International Relations, Department of Political Science of Faculty of Social Sciences, University of Benin, Benin City, Edo State.

_____ _____

DR. AKPOMERA **DATE**

(THESIS SUPERVISOR)

_____ _____

DR. **DATE**

(HEAD OF DEPARTMENT)

_____ _____

(DEAN OF DEPARTMENT) **DATE**

DECLARATION

I hereby declare that this thesis is a study undertaken by me, Tooya Excel Obasi, of the Department of Political Science, Faculty of Social Sciences, University of Benin, under the supervision of Dr. Akpomera and has not been presented in any other institutions. All ideas are product of my personal research and all sources used by other authors have been duly acknowledged.

Student's Signature

…….

TOOYA EXCEL OBASI.

DEDICATION

This work is dedicated to God Almighty. I thank God for making it possible for me to realize this academic desire.

To my family for their incredible understanding, encouragement, patience and support for me at all times.

To Late Mr Anyi Agwudagwu, I am indeed grateful and I appreciate him for always being a source of inspiration, support and encouragement to me all through the course of writing this thesis and to his wife, Mrs Agwudagwu, I remain ever grateful.

ACKNOWLEDGEMENT

I wish to express my profound gratitude first to God Almighty for enabling me in completing this thesis and for his grace and wisdom which he has given to me for this thesis work to be a success. This thesis would not have been a success if not for the guidance and contribution of my thesis supervisor, Dr. Akpomera whose supervision was both as a supervisor and a father, giving advice in ensuring this work came out best.

I wish to extend my gratitude to my family, Mr and Prof. Mrs Obasi and Chineme D. Obasi for their support, encouragement and patience towards me in my struggle towards the realization of my academic pursuit. I also wish to acknowledge my wonderful H.O.D, Dr. Aihie and the staff of the wonderful Department of Political Science.

To a role model, a father and a guardian, Late Mr Anyi Agwudagwu, I say a big thank you for your support in every possible way and to your family I remain grateful.

I modestly wish to thank my grand-parents. I honestly thank Mr and Mrs Aneke, Mr and Mrs Okpunwa, Mr Peter Aneke, Ms Annie Aneke. Mr Greg Obasi, Mr Ben Obasi and their families I say a special thank you for your encouragement. To my friends and course mates who contributed marvellously during my study, thank you and God's grace.

ABSTRACT

This study sought to examine the role of social media and cyber technology in the Russian interference in the 2016 U.S. Presidential Election. The research was prompted by the significant attention and concern surrounding the issue, as well as the complexity and consequences of the problem for both domestic and international politics. The research objectives included a critical analysis of the legality of foreign interference in domestic elections under international law, an examination of the underlying motivations for the Russian interference, an assessment of the effects of election interference on state relations and political processes, and the development of recommendations for reducing the likelihood of similar interference in future elections. The study employed a multi-disciplinary approach, drawing upon a wide range of relevant secondary sources of data such as books, newspaper reports, articles, journals, reports, publications, magazines, commentaries and conference papers. Other sources of data for the research thesis also include internet materials with information relevant to the study to provide a comprehensive understanding of the issue. The findings of the study revealed that Russia's interference in the 2016 Presidential election constitutes a violation of state sovereignty and the principle of non-interference. Furthermore, the study identified a range of factors that motivated the Russian interference, including geopolitical context, domestic political context, and strategic objectives. Additionally, the study highlighted the crucial role that social media and cyber technology played in facilitating the interference and the negative impact it had on political processes and state relations. The study concludes by providing recommendations which include that governments should develop stronger cybersecurity measures and protocols, social media companies should implement measures to increase transparency and accountability, governments should increase international cooperation and coordination, governments should address underlying geopolitical and domestic political factors, and there should be encouragement of the development of critical thinking and media literacy skills in the general population in order to safeguard the integrity of future elections and address the ongoing challenges posed by cyber interference in politics.

KEYWORDS: Social media, Cyber technology, Election interference, Sovereignty, International law.

Word Count: 327

TABLE OF CONTENTS

CHAPTER THREE

METHODOLOGY

CHAPTER FOUR

PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONAND RECOMMENDATIONS

CHAPTER ONE

1.1 BACKGROUND TO THE STUDY

America became a "hyperpower" with the fall of the Soviet Union (Sospedra; 2018). Since then, US relations with Russia have gone through two distinct stages. During the first stage, which Mearsheimer refers to as the "Golden Age," which lasted from 1990 to 2008, the West and Russia coexisted peacefully with the exception of the Balkan Wars, which did not actually pose a threat of war between the two. According to Mearsheimer, there are two fundamental causes for this finding.

The North Atlantic Treaty Organization's (NATO) continued to exist, which accounts for the first reason. Europe continued to be one of the United States' primary international focus areas, which meant that it was established as an arbitrator and the supreme authority that upheld the peace in the region. This reduced the likelihood of confrontation between Russia and European nations, which was beneficial for both.

The second reason however, is that while Russia opposed the first two rounds of NATO expansion, there is little evidence to suggest that the West posed a significant threat to Russian interests via NATO during this period (Sospedra, 2018). Furthermore, the possibility exists that Russia did not view the expansion as an "existential threat", which could explain why the expansions were not perceived as "deadly danger" by Russia. The reasons behind Russia's opposition to the expansion may be rooted in other factors such as concerns about the erosion of its traditional sphere of influence.

However, the second stage is defined as lasting from 2008 until the present. The crucial year for comprehending the deterioration of ties not only between the United States and Russia but

also between Russia and the European Union is 2008. However, abrupt transitions do not occur frequently in the tale; rather, they generally mark the end of an earlier phase.

In the wake of the collapse of the Soviet Union and the termination of the Warsaw Pact, Russia's relationship with the West underwent significant changes. One notable event in this context was President Putin's address at the Munich Security Conference in 2007, in which he outlined his political stance and articulated his goal of restoring Russia's status as a leading force recognized by the West. In this address, Putin criticized the unipolar world led by the United States as being "contrary to democracy" (Sospedra, 2018) and argued that the West had violated commitments made following the collapse of the Berlin Wall by expanding NATO in consecutive waves. This speech is often cited as a reflection of Putin's ambition to re-establish Russia's global power and influence.

The major events however began to unfold in 2008, particularly at the NATO Summit held in Bucharest in April. The main topic of discussion at the summit was the potential membership of Ukraine and Georgia in the Alliance. Despite the fact that these countries did not ultimately gain membership at that time (Sospedra, 2018), there were clear statements made at the summit indicating support for their potential membership, such as "We have agreed today that these countries will become NATO members," "The Membership Action Plan (MAP) is the next step for Ukraine and Georgia on their way straight to the entrance," and "We support the requests of these countries for the MAP" (Sospedra, 2018). The MAP is a program designed by NATO to assist countries in their aspirations to join the alliance. Despite fierce resistance from Russia, NATO moved forward in its support of Ukraine and Georgia's potential membership.

The founding of the Eastern Partnership of the European Union in May 2008 was another significant occasion. This fact demonstrated the European Union's desire to enlarge its

territory to the east (Ukraine). The battle between Russia and Georgia started three months later. This truth will serve as NATO and the European Union's first warning (Sospedra; 2018).

Russia and the United States have historically had a power struggle and rivalry, which has influenced their relationship dynamics. However, this is related to how neorealist thinkers have examined the global order. Neorealist theory holds that the international system is by its very nature anarchical and that this is unavoidable because there is no sovereign authority to oversee and regulate nations' interactions with one another. This idea was put out by Hans Morgenthau in 1985. (Kegley, 2007). This makes specific interests vital in interstate relations, and governments are forced to gain authority in order to actualize and fulfil these interests. Competition in international relations is inevitable due to conflicts of interest and power struggles. In other words, "the idea of interest articulated in terms of power" is the key marker that directs interstate interactions (particularly between great powers) (Morgenthau, 1985). Because of this, Morgenthau came to the conclusion that "power is always the immediate aim in international politics, whatever the ultimate goals may be" (Morgenthau, 1985). Therefore, a "distinguishing aspect of international politics, as of all politics, international politics is of necessity power politics" is the desire and quest for power (Morgenthau, 1985). One can better comprehend the complexities of US-Russia relations in light of this realist and neo-realist analysis. Simply put, the whole relationship between the United States and Russia is defined by the competition for dominance. In contrast to the United States, which wants to maintain the status quo and prevent any prospective power from challenging its "presumed hegemonic" position in international affairs, Russia wants to make its presence felt and tip the scales back in her favour. As a result, there are now more tensions and suspicions about whatever the other party does.

Russia has a long history of vying for control and influence in international affairs, especially in opposition to the United States. This ambition for power dates back to the Cold War, when

the United States and Russia competed for global supremacy. Russia has constantly attempted to put the United States to the test in a number of ways, including by enhancing its military prowess and pursuing influence through political and economic manoeuvres in many parts of the world.

Russia's ambition to re-establish itself as a significant global force, particularly in relation to the United States, is a significant driver behind its foreign policy. This ambition is rooted in the fact that following the collapse of the Soviet Union in 1991, Russia lost its position as a superpower and has since been forced to play a less active role in world affairs. In an effort to reclaim its status as a significant global actor, Russia has been working to strengthen its military and economy in recent years. One of the main reasons for this is the potential for countries like Ukraine, Russia's closest neighbour, to join NATO, which would put Russia at a strategic military disadvantage. This is because Russia's military capabilities would be limited by the proximity of NATO member countries, potentially allowing for a faster and more effective response in the event of any aggression towards Russia. Furthermore, Ukraine's membership in NATO would also give the Alliance access to the Black Sea, which is a major strategic waterway for Russia.

Russia's ambition for power against the United States is also motivated by its desire to defend its national interests. Since the beginning, Russia has been apprehensive of the United States and its allies because it sees them as a danger to its security and sovereignty. As a result, in order to compete with the U.S. and its allies, Russia has worked to improve its military capabilities and forge partnerships with other nations.

The desire for power and influence is a prevalent aspect of international relations, and it is not exclusive to a particular nation or state. In this context, Russia's ambition to assert its power and influence over the United States is driven by a complex set of factors. These

factors have led Russia to adopt a variety of traditional and unconventional methods to obtain and display its dominance. However, it is important to note that the United States, like any other country, has also been known to engage in similar practices, particularly in terms of interference in other countries' politics.

One of the most notable examples of this is the Edward Snowden SAGA, which revealed the extent of the National Security Agency's (NSA) surveillance activities, including the monitoring of foreign leaders and citizens (Greenwald, MacAskill, & Poitras, 2013). Additionally, the United States has been accused of interfering in the domestic politics of other countries, such as the CIA's involvement in the 1953 Iranian coup d'etat, which helped to overthrow Iran's democratically elected government and install the Shah as a US-backed dictator (Kinzer, 2003). Furthermore, the US has been accused of interference in Latin American countries' politics, particularly in countries like Chile, Nicaragua, and Venezuela, through covert operations and support for anti-Communist dictators (Kornbluh, 2013; Grandin, 2006).

While Russia has been accused of influencing political discourse, policymaking, and electoral processes in the United States and other nations, particularly those in Europe and Africa, using a variety of methods such as cyber capabilities and social media (Bowen & Welt, 2021). Russia (or, during the Cold War, Soviet) influence operations meant to meddle in their domestic affairs have been a problem for many governments for years (Bowen & Welt; 2021). According to some scholars, Russia regards influence operations, such as misinformation and propaganda, as a crucial weapon in foreign policy and as a part of a larger rivalry with its alleged adversaries (Bowen & Welt; 2021). Some claim that Russian officials want to meddle in those nations' political processes because they perceive that Russia itself is the subject of internal intervention by democratic foreign powers (Bowen & Welt; 2021). Russian influence operations may aim to weaken societal cohesiveness, generate discontent with democracy and

Western institutions, and encourage political parties and candidates that want closer links with Russia or advocate for policies that serve Russian interests (Bowen & Welt; 2021). However, it is important to note that other nations and actors, including the United States, have also been known to engage in similar practices.

In addition to the various methods of interference in other countries' politics, it is also important to note the role of media and non-state actors in Russia's influence campaigns. According to some scholars, Russian government-funded television and internet news channels such as RT and Sputnik have been identified as major vectors for disseminating influence campaigns directed towards international audiences, with a local-language presence in several nations (Bowen & Welt; 2021). Furthermore, Russia has also been known to utilize non-state actors, such as the Internet Research Agency, to carry out its influence activities (Bowen & Welt; 2021).

Researchers have also observed that increasingly common "homegrown" disinformation operations have the potential to spread Russian narratives or misinformation or promote narratives that support Russia's interests (Bowen & Welt; 2021). It can be challenging to identify players, who are spreading certain narratives on social media, blogs, and messaging services, as well as to trace the sources of these narratives and to distinguish between domestic and Russian-backed misinformation.

Although they frequently take place during election cycles in the targeted nations, Russian influence operations also happen frequently. For instance, a number of Russian media outlets claimed that the 2019 fire at France's Notre Dame Cathedral was the result of an arson attempt by Islamists, the Yellow Vest movement, Ukraine, and the French government itself (French officials said the fire accidentally broke out during construction). A 2016 story that was supported by Russian media that a 13-year-old Russian-German girl had been raped by

migrants in Germany is another often cited case. The claim sparked protests against immigrants and German Chancellor Angela Merkel's immigration policy in Germany before it was shown to be false (Bowen & Welt; 2021).

A declassified intelligence community (IC) assessment on Russian actions and intentions in connection with the 2016 U.S. presidential election was made public by the Office of the Director of National Intelligence on January 6, 2017. The Federal Bureau of Investigation (FBI), the National Security Agency, and the Central Intelligence Agency all stated in the report that they had "high confidence" that President Putin "ordered an influence campaign in 2016 targeted at the US presidential election" in order to "undermine public faith in the US democratic process, denigrate Hillary Clinton, and erode her electability and potential presidency." (Bowen and Welt; 2021).

According to the investigation, the Russian government "aspired to enhance President-elect Trump's election chances by disparaging Secretary Clinton and openly contrasting her to him" whenever this was feasible. Around June 2016, allegations of Russian interference first surfaced (Bowen & Welt; 2021). The Russian government illegally obtained and permitted the distribution of emails and data belonging to the Democratic National Committee as well as emails belonging to Clinton's campaign chairman, John Podesta, according to statements made subsequently by the U.S. intelligence community. WikiLeaks, which is said to have gotten information from individuals with ties to Russian intelligence, released the majority of the emails that were made public. Other emails and files were made public by online users posing as Russian intelligence agents (Bowen & Welt; 2021). According to Bowen & Welt (2021), these activities were allegedly a part of larger collecting attempts against the Democratic Party.

The alleged interference of Russia in the 2016 United States elections has been a source of concern and controversy. While it is acknowledged that Russia engaged in efforts to influence the election, such as through the use of social media and internet propaganda, the Mueller Report concluded that there was no evidence that Russia's efforts extended to actual manipulation of vote totals (Mueller, 2019). Nevertheless, the perception of Russian meddling in the electoral process has had several negative impacts. Firstly, it has raised doubts about the legitimacy of the voting process and has contributed to a decline in public trust in the government. Additionally, it has further exacerbated political divisions and discord within the United States. Moreover, the allegations of Russian involvement have also strained relations between the United States and Russia.

With the growing body of data that indicates social media platforms like Facebook and Twitter had an important influence in the presidential election that took place in the United States in 2016. Russian operatives used these platforms to spread disinformation and sow discord among the American electorate (Bubeck and Marinov, 2019). The role of social media in election interference has become a contentious and difficult topic to fully understand. On the one hand, social media platforms offer a useful service by bringing people together and making it possible for them to exchange information with one another. On the other side, the same platforms may be utilized to disseminate misleading information and take advantage of loopholes in the voting system.

The issue that has to be addressed in this study is the role that social media and cyber technology played in Russia's meddling in the 2016 presidential election in the United States. Despite the fact that this subject has received a lot of attention, there is still a paucity of knowledge on the precise methods and tools that Russia utilized, the degree to which they were successful in influencing the election, and the longer-term effects of their usage. By performing a thorough review of the data that is now available and investigating the effects of

Russia's influence on the integrity of democratic processes and the use of technology in political campaigns, this research seeks to close this knowledge gap. These issues will be addressed in this study, which will offer significant new understandings of a significant recent historical event and contribute to current discussions about the place of technology in society. This study examines the legality of election interference under the international law. The study attempts to explicate the motives behind Russia's interference in the U.S 2016 election. The study examines the role of social media and cyber technology in the election interference addressing the methods utilized and why social media platforms proved to be good tools for the job. The study then goes further to explicate the effects election interference has on state relations and political processes. Finally, the study offers potential recommendations for the prevention of future occurrences of election interference.

1.2 STATEMENT OF THE PROBLEM

There has been a lot of attention and concern about how social media and cyber technologies contributed to Russian meddling in the 2016 American election. In the run-up to the election, Russian agents utilized social media platforms like Facebook and Twitter to spread disinformation and influence public opinion, as shown by the indictment of 13 Russian nationals by the U.S. Department of Justice (2018). The estimated 126 million people who were exposed to Russian propaganda on Facebook alone show how successful these efforts were (Zuckerberg, 2017).

Election meddling caused by the use of social media and other cyber technologies raises complicated issues that go beyond electoral politics. "Election manipulation through social media can be more pernicious than direct tampering with voting machines since it's much harder to detect and resist," writes Hany Farid, a computer science professor at Dartmouth

College (Moses, 2018). Additionally, the adoption of such strategies erodes public confidence in democratic institutions and threatens the fairness of the political process.

Significant repercussions for U.S.-Russia relations have also been caused by Russian interference in the 2016 American election. The Russian government attempted to meddle in the election, as judged by the U.S. intelligence community, in order to harm Hillary Clinton's prospects and increase those of Donald Trump (Office of the Director of National Intelligence, 2017). An already rocky relationship between the two countries has become even more strained as a result of this involvement.

It is crucial to further investigate the role of social media and cyber technology in the Russian meddling in the 2016 U.S. election given the complexity of the problem and its consequences for both local and global politics. Such a study may help guide efforts to safeguard the integrity of next elections and solve the ongoing problems brought on by cyber interference in politics.

1.3 OBJECTIVES OF THE STUDY

Specifically, the objectives of this study can be written as

1. To investigate what the international law says about the legality of a country's Interference in the domestic elections of another country.

2. To examine the reasons behind the Russian interference in the United States' 2016 Presidential election.

3. To probe the role of social media and cyber technology in the 2016 U.S. Presidential Election interference by Russia?

4. To investigate the effects of election interference on State relations and political processes

5. To recommend ways by which election interference between countries can be reduced.

1.4 RESEARCH QUESTIONS

Therefore, this research work shall answer the following questions;

1. What does international law say about the legality of a country's interference in another country's domestic election?

2. What were the motives behind the Russian interference on the U.S. 2016 Presidential election?

3. What role did social media and cyber technology play in the 2016 U.S. Presidential Election interference by Russia?

4. What effects does election interference have on state relations and political processes?

5. In what ways can future election interferences between countries be reduced?

1.5 SIGNIFICANCE OF THE STUDY

Given that there has been consistent increase in election interferences globally and with the Russian interference in the U.S 2016 Presidential election, this research is critical. The fast change in the political domain facilitated by social media to a considerable extent has also made a detailed empirical study of this topic imperative.

This research is critical to

- Academic Institutions; social media has aided in the advancement of learning approaches. These strategies involve the use of electronic devices such as computers, printers, laptops, and other similar devices that help learning and provide a foundation for comprehending new technical processes that will benefit students academically. It

has also revolutionized the process of knowledge acquisition as well as dissemination. This study would provide the academia with sufficient understanding of the role of social media in Russian 2016 interference in the United States' Presidential Election.

- Social media companies have provided a simple and accessible communication network which has contributed a great deal to the human society in various ways including the political sphere by facilitating ease of information dissemination. On this note, the findings made in this study would provide social media companies with practical suggestions on preventing the use of their platforms for election interference purposes.
- Government; in terms of governance, social media has significantly enhanced our system in terms of relationship consolidation between the government and citizens by encouraging increased political involvement among citizens and offering a platform for the government to examine citizens' perspectives. Hence this study would assist the government in making adequate policy decisions to help prevent future election interferences.

1.6 SCOPE AND LIMITATIONS OF THE STUDY

This study focuses on the role of social media and cyber technology in the Russian Interference in the 2016 United States' Presidential election. The research study will cover areas of social media regarding how it contributes to election interference, as well as why it serves as a good tool for interfering in the election process.

Some limitations to the study include;

1) Limited time to carry out research.

2) Insufficient funds.

1.7 OPERATIONAL DEFINITION OF TERMS

Social Media: Social media are internet or electronically driven communication tools that allows for the speedy interchange of ideas, opinions, and information via web-based software or applications on internet enabled devices such as computers, tablets, or smartphones.

Social Networking Sites (SNS): A Social Networking Sites are online platforms that allow users to build individual public profiles, engage with real-life friends, and meet other people based on shared interests.

Election Interference: is the deliberate attempt to disrupt or influence the results of an election. There are a lot of different ways that interference may be carried out, including hacking, voting suppression, voter fraud, and disinformation campaigns.

CHAPTER TWO

LITERATURE REVIEW

2.1 BACKGROUND OF ELECTION INTERFERENCE

Foreign policy has historically included election meddling as a tool. Elections are intricately tied to foreign relations, despite the widespread misconception that they are only domestic affairs. Strong incentives exist for electoral interference since various candidates and parties may have significantly divergent positions on matters that impact third parties or other state actors. For this reason, throughout the last several decades, states have frequently tried to influence the results of elections in other nations (Ohlin, 2020).

Election interference is described by Bubeck and Marinov as "an intentional attempt by a foreign authority to modify the electoral rule or the election outcome" in their book *Rules and Allies* (Bubeck and Marinov, 2019). Bubeck and Marinov divide electoral interventions into two kinds, as implied by this definition:

1. Candidate interventions and

2. Process interventions (Bubeck and Marinov; 2019).

States can combine these strategies to achieve their objectives, influencing the popularity of certain candidates, the election's procedures, or both. According to the authors, there are two basic justifications for state interference in elections: normative preferences for democracy and practical geopolitical considerations (Bubeck and Marinov; 2019). In their sample of elections held after World War II, they discover that interference with elections occurs in around 65% of cases (Bubeck and Marinov; 2019). Election interference has been a typical occurrence in recent history, especially during times of great power struggle like the Cold War, according to the majority of researchers (Ohlin; 2020).

According to research on election interference, the attraction of intervention is dependent on the target state's political division and strategic value to the intervener. Unsurprisingly, states that are strategically significant to the intervener appear to have a higher likelihood of experiencing electoral interference (Bubeck and Marinov; 2019). Additionally, it is generally accepted that political division will encourage nations to interfere in elections (Bubeck and Marinov, Johnson; 2019). The more the candidates' policy stances diverge, the more an intervener can change the outcome. In polarized elections, the gap between candidates is typically wider. Political polarization can facilitate meddling in elections by making it simpler (Johnson; 2019). Opportunistic politicians strive to align themselves with outside players in many divided nations in exchange for support, making it simpler for interveners to advance particular policy results (Ornstein; 2019). Given that Donald Trump explicitly requested Russian assistance during the 2016 U.S. election; this dynamic may have fostered involvement (Ohlin; 2020). Overall, the body of research indicates that when the target is strategically significant and politically divisive, election intervention will be tempting.

Bubeck and Marinov contend, however, that some governments' moral desires for democracy force them to interfere in elections in which they have little geostrategic interest. Sometimes, these conflicting objectives might result in apparently illogical policies (2019). For instance, in the latter days of the Mubarak dictatorship, the United States supported democratic groups in Egypt while also funding a totalitarian state that was actively suppressing them (Bubeck and Marinov; 2019). The American administration attempted a process intervention that benefited the opposition and a candidate intervention that backed the incumbent in an attempt to improve democracy while maintaining its geopolitical interests.

For other practical reasons as well, states frequently decide to strike a balance between procedural and candidate interventions. If a state wants to assist a challenger in unseating an incumbent, for instance, it could work to foster a fair election process even if it has no

inherent support for democracy (Bubeck and Marinov; 2019). Given that eliminating prejudice "makes the link between the support for a certain candidate among the electorate and the final vote share more direct," using this strategy in conjunction with support for a certain candidate is frequently successful (Bubeck and Marinov; 2019). If the electoral process is fair, every dollar spent in support of a candidate will thus have a greater impact. More broadly, in order to optimize its efficacy, election interference is typically carried out concurrently utilizing a number of strategies (Ohlin; 2020). States could, for instance, back adversarial candidates in an effort to split the opposition to the candidate they like. This strategy was used by Russia during the 2016 American election, when it backed Bernie Sanders in an effort to sway voters from Hillary Clinton (Ohlin, 13). Given that each method of election intervention tends to have declining returns, this mix of approaches makes logical.

2.2 THE NEW DYNAMICS OF ELECTION INTERFERENCE: Cyber Election Interference

Cyber election interference is the term for the use of digital technology to disrupt or influence an election's results. This might involve a variety of strategies, such as hacking into voting machines, disseminating false information online, or influencing public opinion on social media. The possibility of cyber election tampering has elevated to a top worry for governments and election authorities worldwide due to the growing dependence on technology in the voting process. Numerous incidents of cyber election meddling have occurred in recent years, including efforts to meddle in the 2016 US presidential election and the 2018 Mexican presidential election. This kind of influence can have far-reaching effects and be detrimental to the democratic process' integrity. Understanding what it is and how it differs from other forms of cyberattacks is so vital. According to Jacqueline Van De Velde (2017), the occurrence of cyber meddling is not new, however, what sets cyber election interference apart from other cyberattacks include the following;

(i) The form of attack,

(ii) What constitutes the target?

(iii) The nature of damage done, and finally

(iv) The absence of a suitable remedy, either under international law or under domestic law.

(i) The Form of Attack

Election-related cyberattacks are similar to other well-known cyberattacks in various ways. Cyber involvement in elections, however, is unique in one important way: it includes both hacking and information dissemination. In the past, most cyberattacks that nations have experienced have mostly entailed kinetic damage to a specific physical object. It is innovative to target and influence civilian hearts and minds through cyber operations of another state.

However, cyber election interference has traits in common with conventional cyberattacks, despite the fact that the stakes are higher in the context of elections. Cyber-attacks are typically invisible, which presents questions concerning

(a) Detecting them as soon as they happen and

(b) Accurately attributing them to the perpetrator so that appropriate sanctions and compensation may be sought.

Being unaware of the attack's timing and the hacker's identity raises specific issues in the context of elections. Firstly, because elections take place at a specific time, it is essential to spot security flaws and inappropriate effects as soon as they are introduced. A crisis of constitutional dimensions may result from the issue being discovered later. For instance, a belated admission that the votes were incorrectly counted and that the win should have gone to another candidate would raise issues much more significant than those in Bush v. Gore. In

reaction to Russian meddling in the U.S. elections, one security expert questioned, "What better method to destabilize a country without a shot being fired?" (Lily; 2016)

Second, the complex problem of tracking down hackers is made considerably more worrisome in an international setting. If international law does address cyber election interference, nations cannot demand compensation or exact retaliation without knowing I who the perpetrator is and (ii) whether or not the perpetrator was under state control. In the situation of cyber election intervention, neither of those qualities is very evident, but the stakes are higher since election interference may have more serious implications than a breach in the commercial sector.

(ii) What Constitutes the Target?

States have utilized lines of code to harm, destroy, or make a piece of equipment in another state malfunction for the attacking state's benefit in prior cyberattacks that worked very similarly to kinetic attacks. Some of these advantages have arisen out of military necessity, such as the suspected hacking of the Iranian centrifuge system by the United States in order to buy more time to negotiate a nuclear deal that would serve the interests of the United States (Langner, 2011). Other cyberattacks have targeted private companies as meager revenge, such as North Korea's efforts to hack and damage the Sony computer system in order to get personal retribution for the release of a movie insulting to North Korean officials (Clapper, 2015).

At least two things make cyber election intervention unique. To begin with, the objectives are publicly held rather than privately owned. Therefore, any assault on a state organ raises concerns about possible violations of sovereignty, both in the broad sense of a state's essence and in the specific sense of boundary and territorial violations.

A few of the targets aren't computers, which is a second and clear point. They are countrymen. In contrast to Stuxnet or the Sony breach, the invasive piece of data is propaganda, intended to effect people rather than computer systems. Regardless of its veracity, information is spread to alter how a sovereign's population behave and harm the state. Election-related cyberattacks are unique from other types of cyberattacks since they directly affect the state apparatus and its population as their objective.

(iii) The Nature of Damage Done

The extent of the impact from cyber electoral tampering might be incomparably greater than that of an assault like Stuxnet. Compare this to Stuxnet, where the harm was initially limited (at least) to the centrifuges used in the Iranian nuclear program. However, there is a chance that cyber electoral intervention will have a far wider impact. It may be possible to limit a hack of a state's voting system to its actual computer infrastructure, but it is more challenging to map or quantify the spread of false information to sway public opinion.

Additionally, if exposed, election-related cyber intervention has the potential to erode public trust in the democratic system and in the reliability of their government. Cyber election meddling prevents people from actively participating in the sort of governance they like. A democratic government is jeopardized if its citizens are unable to effectively engage in it.

(iv) The Absence of a Suitable Remedy, Either under International Law Or Under Domestic Law

Hacks of government systems and assaults on civilians both raise important issues and legitimate worries about unauthorized access to the objects and subjects of state authority. In the real world, when such issues arise, governments do not think twice about waging war to

defend such vital targets. Similar claims are made in the realm of cyber electoral tampering using the same premise.

However, the use of force by sovereigns in retaliation for such incursions is not permitted under international law. The absence of a remedy may encourage governments to (i) employ force without authorization or (ii) expand the boundaries of legitimately applicable international law.

2.3 PROFILE OF THE RUSSIAN INTERFERENCE IN THE UNITED STATES' 2016 PRESIDENTIAL ELECTION

The 2016 Presidential Election in the United States was a highly contentious and polarizing event, featuring two vastly dissimilar candidates who were both met with significant public disapproval. Despite her advantages in terms of experience, political connections, and more traditional views, Democratic candidate Hillary Clinton was widely considered to be the front-runner throughout the campaign. On the other hand, Republican candidate Donald Trump, who had no prior political experience and a tendency towards incendiary rhetoric, was viewed as an unlikely contender. Ultimately, the race for the presidency was highly competitive, with Clinton winning the popular vote by a relatively slim margin (65,844,610 votes to 62,979,636 votes for Trump) (New York Times, 2016), yet Trump emerged victorious by winning the majority of electoral votes (New York Times, 2016). In the early hours of November 9th, major news outlets began to make their predictions on the outcome of the election (Matt and Michael, 2016), ultimately resulting in Donald Trump's ascension to the position of the 45th President of the United States.

On December 9th, 2016, the United States intelligence community verified that the Russian government had actively interfered in the 2016 Presidential Election, in response to the request made by Republican candidate Donald Trump (Sanger and Shane; 2016). This was

further confirmed by a statement by James Comey on June 8th, 2017, which unequivocally affirmed the Russian government's involvement in the hacking of the election (New York Times; 2017). Comey stated that the Russian interference was "very, very serious" and an "assault" on the electoral process (New York Times; 2017).

There is a near-universal consensus among members of the American intelligence community that Russia launched an extensive and aggressive campaign of electoral interference in order to damage the legitimacy of the Democratic candidate Hillary Clinton and heighten domestic political tensions within the United States (Mueller; 2019). This campaign included cyberattacks on the Democratic Party, the spread of false information on social media, and attempted interference with voting systems in all 50 states (United States). The Russian government's efforts have been widely believed to have played a significant role in the unexpected victory of Donald Trump on Election Day, which has resulted in a highly polarized political climate within the United States.

However, some have questioned whether the Russian interference can be considered an "attack" in the traditional sense. While no physical manipulation of voting equipment or casting of false votes was discovered, the extensive use of disinformation and attempts to influence the American public's opinions, votes, and behaviour can be considered as a kind of information warfare (New York Times, 2017). James Comey and Senator Warner have both stated that this constitutes a breach of American sovereignty and that such interference can be considered an attack (New York Times, 2017). Some academics and decision-makers have gone further to assert that such a breach can be considered a sufficient reason for military action.

2.4 THE VIEW OF ELECTION INTERFERENCE FROM THE PERSPECTIVE OF INTERNATIONAL LAW.

As more information regarding the Russian interference in the United States' 2016 Presidential Election has come to light, political officials from both major parties in the United States have referred to the interference as an "act of war." While the concept of election interference may be considered political theatre, it raises the question of how new concepts of cyber warfare apply. This is because cyber warfare is fundamentally different from traditional warfare, which is defined as an armed conflict or physical violence between nations that involves the use of military force.

The principle of the widespread prohibition on the use of force, outlined in Paragraph 4 of Article 2 of the United Nations Charter, is a fundamental aspect of conventional international law that governs the conduct of nations during times of conflict (jus ad bellum). According to Article 2 of the United Nations Charter, all member states "shall refrain in their international dealings from the threat or use of force against the territorial integrity or political independence of any state, or in any other way inconsistent with the goals of the United Nations" (U.N. Charter; 1945). Given the crucial role that elections play in the functioning of a democracy, election meddling could be interpreted as a violation of a country's political independence, although this is a contested view.

The question of what constitutes force in the context of cyberspace also needs to be addressed. The Tallinn Manual 2.0, which is a non-binding but valuable source of research on the subject, states that cyber operations may be considered a use of force in violation of the prohibition if their "size and consequences are equivalent to non-cyber operations reaching to the level of a use of force." This is stated in the context of the prohibition on such activity (Michael; 2017). The Tallinn Manual 2.0 lists factors that states are likely to consider when

determining whether or not force was used, including the severity, immediacy, directness, and invasiveness, measurability of effects, military character, state involvement, and presumptive legality of the action. However, international law does not provide a clear definition of the term "use of force" (Michael; 2017).

Given these considerations and the ambiguity in the definitions, it is uncertain whether Russia's conduct constitutes an act of war under international law. Michael Hayden, a former director of the Central Intelligence Agency, has warned against designating Russian election interference as an "act of war" (Chalfant; 2017). The director of the Tallinn Manual project, Michael Schmitt, has also rejected the idea that this interference constitutes warfare, referring to it as "asymmetrical law fare" in a "grey area" of international law (Michael; 2017). Furthermore, the Tallinn Manual 2.0 concludes that "cyber psychological operations intended solely to undermine confidence in a government... do not qualify as uses of force" (Michael; 2017).

2.4.1 The Russian Interference In The United States' 2016 Presidential Election As A Violation Of The State Sovereignty And The Principle Of Non-Intervention.

Many critics have made the decision to focus their attention on election interference as a breach of state sovereignty and the principle of non-intervention, both of which are fundamental notions that underlie the larger ban on the use of force. In 1965, the United Nations General Assembly reaffirmed the principle of non-intervention by declaring that " no State has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal affairs of any other State" and that " every State has an inalienable right to choose its own political, economic, social, and cultural systems, without interference in any form by another State." (United Nations Charter; 1945) In Nicaragua v. United States of America, the International Court of Justice (ICJ) stated that the principle of non-intervention "is an integral

part of customary international law" (ICJ; 1986) and that it "prohibits all States or groups of States from intervening directly or indirectly in the internal or external affairs of other States." (ICJ; 1986)

The Tallinn Manual 2.0 comes to a conclusion that is quite similar to this one, namely that foreign nations may manipulate elections through cyber methods, "for example, by employing cyber operations to remotely modify electronic votes" (Michael; 2017). Despite the fact that it would appear that Russian interference in the 2016 US election did not materially alter the results, it had a significant influence nonetheless: The Mueller Report claims that computers belonging to state electoral boards, secretaries of state, and American firms that provided software and other technology related to the conduct of U.S. elections were all compromised by Russian military forces. 2017 (Michael) Russia did target election systems in all fifty states, according to a research published by the Senate Intelligence Committee of the United States. Russia "may have been testing flaws in voting systems to exploit later," according to the assessment. 2019 Senate Intelligence Report Although such actions may still be regarded as unlawful interference, the writers of the Tallinn Manual 2.0 did not discuss particularly the sorts of social media influence operations, hacking, or the disseminating of harmful material employed in Russia's 2016 cyberattacks.

The International Court of Justice (ICJ) rendered a decision in the 1986 case Nicaragua v. United States of America (Military and Paramilitary Activities in and Against Nicaragua), which was brought by Nicaragua against the United States of America. The declaration claims that it is illegal under Nicaraguan law for one country to utilize coercive measures, like force, to meddle in another country's internal affairs. This declaration was made as part of the court's decision in this case, which found that the United States had infringed international law by supporting the Contras in Nicaragua and conducting military and paramilitary activities against Nicaragua. According to the International Court of Justice

(ICJ), these actions were a violation of the non-intervention principle, which states that countries shouldn't meddle in the internal affairs of other states. Given that the ICJ agrees that a state should freely select its political system, the more difficult question is what constitutes coercion (ICJ; 1986). Opinions vary on this. Jens David Ohlin, for instance, argues that interference in the 2016 election was not intrinsically coercive since it is hard to pinpoint precise coercion targets or acts that are directly pressured (Ohlin; 2017). Others, however, argue that the interference constituted coercion because of the state interests at stake and the cumulative power of the incursions to alter the outcome of the election (Barela; 2018). Understanding the potentially paralyzing effects of eroding the integrity of American democracy and elections is the crux of "coercion," according to Steven J. Barela (2018). This assertion is based on the Mueller Report's description of the Russian "social media campaign that promoted Donald J. Trump and disparaged Hillary Clinton" (Mueller; 2019). Despite not necessarily viewing Russian interference as a violation of international law, the administration of President Barack Obama expressed a similar understanding, noting that "Russia's cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government." (Obama; 2016) Therefore, if it is believed to be an effort to "provoke and deepen political and social divide in the United States," as the Mueller report puts it, election interference may be regarded criminal activity (Michael; 2017).

It would be necessary for the measures to be deemed an "interference with or usurpation of intrinsically governmental powers" in order for them to qualify as an illegal intrusion in state sovereignty (Michael; 2017). The Tallinn Manual 2.0's authors state that "examples include modifying or deleting data such that it interferes with the conduct of elections" without offering a clear description (Michael; 2017). Again, this is not a precise description of what

transpired in 2016, but the mention of election meddling is relevant given the evidence that Russian operatives had already targeted American electoral systems, maybe as a first step towards directly influencing such data in the future.

On the basis of the aforementioned, it is possible to construct a convincing argument that Russia's actions during the 2016 U.S. elections constituted at the very least an unconstitutional intrusion on American sovereignty, if not a direct act of war.

2.5 THE MOTIVES BEHIND RUSSIA'S INTERFERENCE IN THE UNITED STATES' 2016 ELECTIONS

The interference of Russia in the presidential election of the United States in 2016 has sparked a significant amount of controversy and discussion. It is generally agreed upon that Russia wanted to interfere in the election in order to damage the reputation of the United States of America and pose a danger to its democracy. However, the precise scale of Russia's action and the motivations for Russia's interference remain unknown. Because Donald Trump has previously expressed admiration for Vladimir Putin, the president of Russia, some people believe that Russia may have wanted to assist Donald Trump in winning the presidency of the United States.

For a number of different reasons, it is extremely important to have a solid understanding of the reasons why Russia interfered in the presidential election in the United States in 2016. For instance, having an understanding of Russia's goals might affect how the United States and other countries respond to interference of this kind and how well they protect their democratic institutions. To help restore the prestige of the United States and the democracy it has fostered, it is helpful to get an understanding of the reasons Russia interfered in the U.S. elections.

Although, as noted previously, few assumptions have been made regarding the motivations for Russia's meddling, this study focuses on a few reoccurring plausible elements that may have functioned as incentives for the interference. In doing so, this study summarizes these factors into three major categories:

(i) The geopolitical context of Russia's interference

(ii) The domestic political context of Russia's interference

(iii) The strategic objectives of Russia's interference

2.5.1 The Geopolitical Context of Russia's Interference

As was indicated earlier, Sospedra (2018) asserts that the geopolitical climate in which Russia's interference in the presidential election of the United States of America in 2016 took place was one in which relations between the two countries were already strained. Before the election, many of the most contentious topics between the United States and Russia were the crisis in Syria, the expansion of NATO, and Russian aggression towards states that are geographically next to Russia. Sanctions were imposed on Russia by the government of the United States due to Russia's involvement in the conflict that was taking place in eastern Ukraine and its annexation of Crimea.

Additionally, the victory of Donald Trump was seen positively by Russia as a result of his stated readiness to expand ties and engage with Russia on issues such as fighting terrorism. It was widely believed that Russia's intervention in the election, which included hacking and disinformation operations, was an attempt to aid Donald Trump in his victory and hinder Hillary Clinton in her bid for the presidency (Sanger and Shane; 2016).

In general, Russia's interference in the presidential election in the United States in 2016 took place in the context of preexisting tensions and a desire to advance politically during a contentious race.

2.5.2 The Domestic Political Context of Russia's Interference

By analysing the status of Russian politics as well as the United States' domestic political climate prior to the election and the events that occurred during the election, it is possible to comprehend the domestic political backdrop of Russia's intervention in the U.S. 2016 election.

First of all, it's crucial to remember that Russia has a history of meddling in other nations' internal politics (Bowen & Welt; 2021). This influence sometimes takes the shape of covert operations designed to harm the reputation of targeted countries and their democratic institutions. Russia was apparently involved in a number of these activities leading up to the 2016 U.S. election, including the hacking of the Democratic National Committee's emails and the dissemination of false material on social media (Bowen & Welt; 2021).

Secondly, President Vladimir Putin's administration in Russia was characterized by rising authoritarianism in the run-up to the 2016 presidential election in the United States. Putin had been in power since 2000 and had strengthened his hold on the nation by a number of actions, such as the repression of political opposition and the restriction of civil freedoms. In light of this, it is possible to view Russia's interference in the 2016 U.S. election as an extension of its domestic political agenda (Lewis; 2020).

Thirdly, it is important to note that Russia's interference in the U.S. 2016 election occurred at a time when the United States was experiencing deep political divisions and polarization.

This political climate may have made it easier for Russia to sow discord and undermine trust in the U.S. democratic process (Johnson; 2019).

In conclusion, the domestic political context of Russia's interference in the U.S. 2016 election was one of increasing authoritarianism in Russia, rising tensions between Russia and the United States, and political polarization in the United States. These factors may have played a role in Russia's decision to interfere in the election and contributed to the success of its operations.

2.5.3 The Strategic Objectives of Russia's Interference

Although the precise strategic intentions of Russia's meddling in the 2016 U.S. election are unknown, it is widely assumed that Russia aimed to accomplish a number of objectives with its activities.

First off, it's probable that Russia wanted to harm the United States' reputation and threaten its democracy. Russia attempted to undermine faith in the American democratic system by hacking the Democratic National Committee's emails and disseminating false material on social media. This would have reduced the United States' influence on the world stage and jeopardized its capacity to advance democratic institutions and principles.

The second possibility is that Russia actively worked to support Donald Trump's election as president of the United States. In the past, Trump had praised Russian President Vladimir Putin and supported measures that would benefit Russia, such as removing sanctions and acknowledging Russia's annexation of Crimea. Russia may have believed that by meddling in the election and backing Trump, it would improve ties with the United States and further its own geopolitical objectives.

Thirdly, Russia's interference in the 2016 U.S. election may also be understood as a component of its overarching plan to portray strength and influence on the world stage. Russia wanted to show that it could influence events and threaten the United States' hegemonic position in international affairs by meddling in the election of a major world power like the United States. This would have improved Russia's status and given it more influence in negotiations with other nations.

Finally, it can be said that Russia's strategic goals in interfering in the 2016 U.S. presidential election were likely to harm American reputation, aid in the victory of Donald Trump, and strengthen Russia's position and influence internationally.

2.6 CONCEPTUAL FRAMEWORK

Social media

Social media is a kind of communication in which individuals produce, share, and exchange information and ideas in virtual groups and networks. Furthermore, social media relies on mobile and web-based technology to build highly participatory platforms through which individuals and communities exchange, comment on, discuss, and alter user-generated material (Chiemela, Ovire, Obochi, 2015).

Kaplan and Haenlein (2010) described social media as a collection of Internet-based applications that are based on the ideology and technology of web 2.0 and enable the creation and exchange of information. They refer to internet-based social platforms such as Facebook, MySpace, and Twitter, which allow users to engage with one another in real time.

Election Interference

Election interference is described by Bubeck and Marinov as "an intentional attempt by a foreign authority to modify the electoral rule or the election outcome" in their book *Rules and*

Allies (Bubeck and Marinov, 2019). Bubeck and Marinov divide electoral interventions into two kinds, as implied by this definition; Candidate interventions and Process interventions.

2.7 THEORETICAL FRAMEWORK

This study adopted and employed two theories as framework for our analysis of the Russian interference in the United States' 2016 Presidential election. These theories are;

(i) The Realism Theory

(ii) The Media Effects Theory

(i) The Realism Theory

One of the oldest and best-known theories of international relations, realism bases its justification on ideas of power. The realist school's philosophy, which blames power politics and egotistical state conduct for conflict and violence, is frequently perceived as having a negative outlook on the world. Classical, neoclassical, offensive, defensive, and structural realism are some of the varieties. All of them share the same fundamental premise: States are typically the primary actors in international politics; power and security considerations are crucial; the national interest should guide states rather than sub-national or supra-national interests; the world is dangerous both because human nature is morally corrupt, or at least has an element of evil in it; and because, unlike domestic society, this realm lacks a higher authority that can provide guidance. In this instance, there are a number of sayings that may be quoted, one of which was written by George Washington which states, "It is a maxim founded on the universal experience of mankind that no nation can be trusted beyond the confines of its own interests." (Morgan; 1977)

Persons or groups of individuals are viewed as rational agents who want to maximize their power in order to better their chances of survival in conventional realist thought. People feel

intimidated when someone else is stronger than they are because it presents a security risk. According to Hobbes, the state of nature is "a war of all against all" when there is no central authority to supervise and control the behaviour of people or organizations. In other words, the strong players can dominate and take what they want from the weaker ones in the absence of an absolute sovereign to enforce laws and punish transgression (Forde; 1992). Therefore, in order to assure self-preservation, it is essential to amass as much power as you can. A central governing body that rules over people's self-interested character and conduct is required to provide order and stability. In order to understand state behaviour and global politics, the realism approach to international relations applies these ideas on a global scale.

Three fundamental presumptions form the foundation of the realism theory of international politics. As indicated earlier, the first premise regards nations as the primary actors in international relations and, hence, as the units of study. Therefore, realism is a state-centric ideology. According to the second premise, all governments strive for survival and power growth since it improves their security relative to other states on the international scene (Jervis; 1985). The third premise holds that states are rational actors that thoroughly consider the advantages and disadvantages of an action before acting in order to foresee possible outcomes.

When analysing Russia's interference in the presidential election in the United States in 2016, this study adhered to all three tenets of the realism theory. The most important of these was the second premise, which states that governments on the international stage engage in power politics in order to ensure their own survival. It's possible that Russia decided to interfere in the presidential election in the United States in 2016 so that it might create disruption in the American political system. This would give Russia an edge or a higher chance of dominating the United States and so yet again furthering Russia’s national interests.

(ii) The Mass Effects Theory

The term "media effects" refers to several hypotheses and theories concerning the ways in which audience members' attitudes and perspectives are influenced by the media. One of the most important ideas in the field of communication studies is that of media effects (Neuman & Guggenheim, 2011).

A three- or four-phase paradigm with "significant" or "minimal" media impacts has historically been utilized for media effects (see Bryant & Thompson, 2002; McQuail, 2010; Noelle-Neumann, 1973; Wartella & Middlestadt, 1991). Each phase is defined by new media technology, culture, research procedures, opinions, and ideologies. In the 1920s and 1930s, messengers used metaphors like "magic bullet" or "hypodermic needle" to blast messages and effects into recipients. Media was credited with influencing opinion, attitudes, and behaviour as print, film, and radio grew pervasive. Locals and specialists at this period were concerned about the widespread effects of new media, such as radio and movies. Propaganda strategies used during World War I increased these concerns. Harold Lasswell was the father of media effects (1927). Lasswell made the case using political science, pragmatism, and Freudian psychology that a minority might rule society and the populace through propaganda.

Under the general heading of "media effects," there are several significant hypotheses. To go into detail on all of them would go beyond the scope of this article. These theories include the following;

1. Cultivation theory

2. Exemplification theory

3. Uses and gratifications

4. Third-person effect

5. Effects of media violence

6. Framing effects, agenda-setting, and priming

However, the framing effects, agenda-setting, and priming theories are the most crucial theories among those previously mentioned that are relevant to this study. These three media effects theories are some of the ones that are frequently utilized in the study of political communication. This corpus of work "signalled the most recent paradigm shift in political-communication studies" (Scheufele & Tewksbury; 2007). Given the significance of this field of study, this article concentrates on these three key theories of media impacts and describes the cognitive mechanisms at play in each.

Framing study has yielded much literature. Framing study is interdisciplinary, therefore frame definitions and methods vary (Borah; 2011). “Characteristic of the discourse itself,” frames provide “a basic structural idea” (Pan & Kosicki; 1993, Gamson & Modigliani; 1989), they "draw attention to certain areas of reality while obscuring others" (Cappella & Jamieson, 1997) and "structure on which other components are created" (Entman; 1993). The Framing effect study studies "individual frames" or "mentally stored clusters" (Scheufele; 1999, Pan & Kosicki; 1993). Frames can mean "technology embedded in political communication" or "internal structures of the mind" (Kinder & Sander; 1996). This "double life" (Kinder & Sander; 1996) of framing research may appeal to several disciplines. Thus, conceptual framing is socio-psychological.

The evolution of audience frames and media frames have drawn the most intense research interest. Numerous studies have demonstrated how news framing impacts how information is processed and how decisions are made. Kahneman and Tversky (1979, 1984) demonstrated how different information presentations might influence people's decisions. When "losses" were highlighted, risk-taking rose. When "gains" are offered, risk-taking declines. According

to Kahneman, the "determinants and consequences" of accessibility explain prospect theory, framing effects, and cognitive processes (2003). His guiding philosophy is "passive acceptance of the formulation presented."

According to the "emphasis" (Druckman; 2001) framing effect, drawing attention to certain features of a message may cause it to be remembered. This approach contends that facts can occasionally be changed by manipulating frames. It is true, as Druckman (2001) points out, that it is not always feasible to portray a scenario in a variety of equally valid ways, particularly when dealing with political issues. When people prioritize a group of "potentially essential factors" in their decision-making, emphasis framing effects take place (Druckman; 2001, p. 230). Political framing, then, usually refers to "characterizations" of a line of action where a central idea lends the incident importance (Sniderman & Theriault; 2004).

In reality, agenda-setting and priming have frequently been lumped together with framing studies. The broad category of cognitive media impacts has been studied to some extent for all three strategies (Scheufele, 2000). The three strategies do, however, vary conceptually and practically.

McCombs and Shaw (1972) examined the idea that mass media set the public agenda through daily news selection, challenging the limited effects hypothesis. They identified a strong rank-order link between media and public agenda items. Many research use the procedure. Agenda-setting studies have included framing as a second factor (Maher, 2001). Scholars like Scheufele (2000) have refuted this and described the distinctions between the two processes. The frequency of media coverage sets agendas. It does not affect media coverage or framing (Cappella & Jamieson, 1997).

Priming, like framing, alters the prominence or accessibility of information utilized in judgment or assessment. Iyengar and Kinder describe priming as “the changes in the

standards that people employ to make political evaluations" (1987). Priming research recognizes that humans are cognitive misers who will not and often cannot, analyse all the relevant information before making a choice. Instead, they use a number of heuristics, notably information accessibility, to make their decision (Iyengar & Kinder; 1987). Priming holds that the media prioritize issue significance and utilize it to assess leaders, unlike agenda-setting (Cappella & Jamieson, 1997). Basically, agenda-setting and priming theories focus on news primarily on coverage frequency rather than treatment.

These concepts provide, in essence, a framework for analysing Russia's use of social media platforms to influence the elections that took place in the United States in 2016, as well as the reasons why their efforts may have been effective despite the fact that they were subtle and covert. The assertions made by the framing, agenda-setting, and priming theories regarding the power and strength of media and hence which is similarly portrayed by social media in influencing people's political ideas and choices provide a fundamental illustration of this point. However, because social media platforms provide users the flexibility to create and share their own content, Russian operatives were able to develop and disseminate false information that may have influenced voters' judgments

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The purpose of this study is to examine the role of social media and cyber technology in the Russian interference in the 2016 U.S. presidential election, and to explore how these technologies were used by Russian agents to influence the election.

This chapter will present the research methodology used to answer this research objective. The chapter will begin by providing an overview of the research design. It will then describe the population of the study, the sample size and sampling technique, the sources of data and the data description. The chapter will conclude with a discussion of the method of data analysis employed.

3.2 RESEARCH DESIGN

In order to answer the research questions about the role of social media and cyber technology in Russian interference in the presidential election in the United States in 2016, this study utilized the research technique of document analysis as its primary method of analysis. Document analysis is a research method that entails the methodical analysis of written documents, such as reports, articles, policy documents, and other forms of written communication, in order to identify patterns and themes related to the research questions. This can be done in order to draw conclusions about the topic under investigation. This approach is frequently used in qualitative research designs, the purpose of which is not to test hypotheses or make predictions but rather to get an understanding of the meanings, experiences, and points of view of individuals or groups of people.

The primary focus of the study was on secondary data taken from previously published government reports. The term "secondary data" refers to information that was gathered by a

source other than the user themselves. Reports from the government, polls, and research that has been published are all examples of common sources of secondary data. The choice to use secondary data instead of primary sources was made based on a number of considerations, including objectivity, accessibility, availability, and thorough information. The researcher was constrained by distance, therefore was unable to collect primary data from people living in the United States by conducting interviews or distributing questionnaires to that population. However, the researcher had access to a substantial volume of secondary data on the research subject in the form of reports from the government, which provided a dataset that was both rich and diverse for the researcher to evaluate. In addition, primary data sources may not have had the information that was supplied by official publications, which was extensive and in-depth on the study issue. Finally, secondary data sources were seen to be more objective than primary data sources since the researcher did not have a direct role in collecting them and because they were not affected by the researcher's preconceived notions or prejudices.

3.3 POPULATION OF THE STUDY

The population for this study consisted of all available sources of data related to the role of social media and cyber technology in the Russian interference in the 2016 U.S. presidential election. These sources included academic articles, news articles, government reports, and other forms of written or visual communication that provided relevant information on the research topic. The population was larger than the sample, which was the specific subset of sources that were actually analysed as part of the study.

3.4 SOURCES OF DATA

As they offer the basis for the analysis and findings, the data sources utilized in this study are a key component of the research. In order to accomplish the goals of the research, the study relied exclusively on secondary data that was taken from official government reports. The use

of secondary data, rather than primary sources, was a deliberate decision made by the researcher due to a number of considerations, including the ease of access, the availability of information, the level of detail provided, and the objective nature of the data. This section will offer a complete description of the sources of data that were utilized in the study, including the particular government reports that were analysed, as well as how and why these sources were selected. The study's sources will consist of the five most pertinent government reports to this research study. The following are the;

1. Report on the Investigation of Russian Interference in the Presidential Election of 2016: The Special Counsel's office, which was appointed to examine Russian interference in the 2016 election, published this report, usually known as the Mueller report, in April 2019. The study gives specific details on how Russian operatives used social media and cyber technologies to interfere with the election, as well as suggestions for preventing future interference.

2. Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: This July 2018 report was published by the United States Senate Select Committee on Intelligence. It presents a summary of Russian influence activities, including the use of social media and cyber technologies, and makes suggestions for enhancing the security and resilience of U.S. elections.

3. Report: Statement on Election Security by the U.S. Department of Homeland Security (2017): This report was published by the U.S. Department of Homeland Security in September 2016. It addresses the issue of election security and provides information on the department's efforts to protect the integrity of the U.S. electoral process.

4. Report: Assessing Russian Activities and Intentions in Recent U.S. Elections by the U.S. Office of the Director of National Intelligence (2017): This report was published by the U.S. Office of the Director of National Intelligence in January 2017. It assesses Russian activities and intentions related to the 2016 U.S. presidential election, including the use of cyber technologies and social media.

5. Report: Russian interference in the 2016 U.S. election by the U.S. Department of Justice (2018): This report was published by the U.S. Department of Justice in 2018. It provides information on the Russian government's interference in the 2016 U.S. presidential election, including the use of cyber-attacks and social media.

Purposive sampling, which is a non-probability sampling strategy in which a sample of sources is selected based on their relevance or value to the research objectives, was employed to achieve this sample size. In a purposive sample, the researcher selects sources based on specified criteria or features that are relevant to the research questions, such as sources that are regarded as experts in the field or sources that offer unique or unconventional viewpoints on the study issue. The particular criteria utilized to select the samples for this study are outlined in the following section.

1. Relevance: All of these reports are closely connected to the research subject and contain thorough information on the usage of social media and cyber technologies in the Russian efforts to interfere.

2. Expertise: Since these reports are generated by government entities with expertise in intelligence and investigation, they are likely to provide credible and accurate information on the topic of research.

3. Uniqueness: These studies give unique insights on the Russian interference activities and may provide viewpoints or material not found in other sources.

4. Accessibility: These reports are readily accessible and available to the general public.

3.5 DATA DESCRIPTION

The scope of the data collected and analysed in this study was limited to the specific case of Russian interference in the 2016 U.S. presidential election. The choice of this period of study was based on the increased use of social media and cyber technology in politics globally, as well as the specific event of Russian interference in the U.S. election that year. The sources for the study were selected based on their relevance to the research question and their potential to provide insight into the role of social media and cyber technology in the Russian interference.

The data collected from these sources was analysed using the research method of document analysis. This analysis identified several key themes related to the use of social media and cyber technology in the Russian interference in the 2016 U.S. election. One such theme was the use of fake news and propaganda to influence public opinion and voter behaviour. This included the creation and dissemination of fabricated news stories as well as the manipulation of existing news stories to present a biased or misleading view.

Another theme that emerged from the analysis was the use of bots and automated accounts to coordinate and amplify the efforts of those seeking to interfere in the election. These bots were programmed to promote certain messages or candidates and could create the appearance of widespread support for a particular candidate or issue, even if that support did not actually exist.

A third theme identified in the analysis was the manipulation of social media algorithms to prioritize certain content or to suppress the visibility of other content. This could be done to amplify the reach of certain messages or to suppress the visibility of opposing viewpoints.

The fourth theme regarding the use of cyber technology in the interference identified in the analysis was the use of malware and other forms of cyber-attacks to disrupt election systems. This finding suggests that Russian state-sponsored hackers and operatives used malware and other forms of cyber-attacks to infiltrate American political organizations and compromise voting systems. This was done in an attempt to influence the 2016 U.S. presidential election.

The fifth theme based off the analysis was the hacking of Democratic Party email accounts and the release of stolen information. This finding indicates that Russian state-sponsored hackers targeted the email accounts of the Democratic Party, stealing and releasing sensitive information through WikiLeaks. This was done with the intention of aiding their preferred candidate and influencing the election outcome.

The sixth theme that developed from the analysis was the use of cyber technology to gather intelligence and track election-related activities. This finding reveals that Russian state-sponsored operatives also used cyber technology to gather intelligence and monitor election-related activities. This was done to gain a better understanding of the political landscape and identify vulnerabilities that could be exploited to influence the election.

3.6 METHOD OF DATA ANALYSIS

The study employed the document analysis method as the method of data analysis. Document analysis is a method of analysis that involves the systematic examination of written or printed documents to understand their content and context.

To conduct the document analysis for this study, the following steps were followed:

1. Identification of key documents: The first step in the document analysis process was to identify the key documents to be analysed. This included a review of relevant academic articles, news articles, and government reports related to the Russian interference in the 2016 U.S. election. Of which two key government reports that were of the most relevance to the research questions were selected as the sample for the study.

2. Analysis of the data: Once the key documents have been identified and data has been extracted from them, the next step was to analyse the data to identify patterns and trends and to draw conclusions about the research question. This involved a close reading of the data and a careful examination of the themes and patterns that emerged.

CHAPTER FOUR

THE ROLE OF SOCIAL MEDIA AND CYBER TECHNOLOGY IN THE RUSSIAN INTERFERENCE IN UNITED STATES' 2016 ELECTION

4.1 INTRODUCTION

Russia's tactical utilization of social media and other cyber technologies had a significant impact on the outcome of the presidential election in the United States in 2016. The goal of these strategies was to influence public opinion and disseminate false information in order to influence the outcome of the election, and it is widely assumed that the Russian government was behind their implementation. Through the dissemination of false news items and targeted ads, Russian agents were able to sow dissension and doubt among American voters during the 2016 presidential election. In addition, they disclosed sensitive material that they had obtained from the email accounts of high-ranking officials in an effort to further undermine the legitimacy of the voting process. This highlights the need for increased precautions to prevent foreign interference in future elections and demonstrates the significant impact that social media and cyber technology can have on political events.

It is possible that the use of these technologies to meddle with elections may disrupt democratic processes and impair international relations. Because of this, discussions concerning the relationship between election meddling and state relations are still going on today. While there are many who believe that interfering in the political processes of other nations constitutes a breach of international law, there are also those who believe that such behaviour falls within the bounds of acceptable statecraft. Regardless of where one stands on the issue, it is abundantly evident that further monitoring measures are required to exclude the possibility of future elections being swayed by governments located in other countries.

It is important to note, however, that Russian President Vladimir Putin has denied any involvement in the presidential election that took place in the United States in 2016. Putin

stated that "We never engaged in it on a governmental level, and have no intention of doing so." (Tass, 2017). The Russian intelligence agencies have also denied any participation, with the Federal Security Service (FSB) declaring in a statement that was released in 2017 that "The FSB has not carried out any cyber assaults on the email accounts of officials from the US Democratic Party" (Tass, 2017). In spite of these denials, several investigations, including those conducted by the United States Intelligence Community and by Special Counsel Robert Mueller, have revealed evidence of Russian meddling in the election of 2016 through the use of social media and cyber technologies.

There are several compelling reasons why there should be an immediate investigation into the role that social media and other forms of cyber technology played in Russian interference in the presidential election of 2016. To begin, it could be to everyone's advantage to have an understanding of the strategies and procedures that the government of Russia uses in order to stop interference of this kind in next elections. The people and their governments have the ability to protect the democratic process from meddling from the outside world and preserve its fundamental integrity by engaging in self-reflection and making use of the insights gained from mistakes made in the past. Second, doing study into the effects that social media and cyber technology had on the presidential election of 2016 can provide information into the ways in which these technologies influence political discourse and decision-making more generally. This might be helpful in directing tactics and regulations that aim to reduce any potential negative impacts that social media could have on political processes. In conclusion, doing study on the ways in which social media and other cyber technologies influenced the presidential election in 2016 will assist us in gaining a better understanding of the opportunities and challenges that these technologies bring in the twenty-first century.

The purpose of this chapter is to analyse the role that social media and cyber technology played in the interference as two different but linked parts of the jigsaw puzzle in order to

address the problem that has been brought to our attention. Analysing each of their functions and illustrating how the organism as a whole utilized both of them in ways that complemented one another to achieve its goals. This study goes further to identify and completely define the technique and tools that were used, putting particular emphasis on the dangers associated with specific technological systems. This Chapter also goes further to address the effects that election interference has on state relations and political processes.

4.2 WHY ARE SOCIAL MEDIA AND CYBER TECHNOLOGY EFFECTIVE TOOLS FOR ELECTION INTERFERENCE?

The ways in which we connect with one another and gain access to information have been fundamentally transformed as a result of the rise of social media and digital technology, but these developments have also ushered in a host of new chances for malicious electoral meddling. The ability of these tools to reach and influence large numbers of people, the use of targeted advertising and micro targeting, the use of hacking and cyberattacks, and the ability to interfere in elections without being detected are the characteristics that have made these tools great tools for election interference (Woolley and Howard 2016).

(i) **The ability to reach and influence large numbers of people**

One of the most important qualities that gives social media and cyber technology their effectiveness as instruments for election intervention is their capacity to communicate with and sway vast populations of individuals. Social media platforms like Facebook and Twitter each have billions of users, which means that they offer access to a sizable audience to anyone who wish to spread misinformation and false information. This is of particular relevance in the context of elections, given that one's capacity to communicate with a big number of individuals in a very short period of time has the potential to have a sizeable impact on the final tally of votes cast.

One illustration of this is how misleading information and misinformation were disseminated over social media platforms during the Brazilian presidential election of 2018. According to a survey published by the Oxford Internet Institute, a substantial portion of the misleading material that was spread over social media during the election was focused at smearing the reputation of Fernando Haddad, the candidate of the Workers' Party (Oxford Internet Institute, 2019). This misleading information was able to spread to millions of people in a very short period of time, and it is possible that it contributed to the election of Jair Bolsonaro as president of Brazil.

One further illustration of this is the utilization of social media in the presidential election of Kenya in 2017. According to the findings of a research conducted by the Pew Research Center, an overwhelming majority of Kenyans (87%) had access to the internet, and a significant proportion of those internet users (80%) utilized social media platforms such as Facebook, WhatsApp, and Twitter (Pew Research Center, 2017). Because of this, it became easy for incorrect information to be exchanged and fast disseminated across the community. According to the findings of the investigation, misleading material was also spread in an effort to sway public opinion and tilt the results of the election.

These instances demonstrate the ability of social media to reach and influence vast numbers of people, as well as the possibility that this power may be exploited to meddle in electoral processes. It is very necessary to take measures to prevent the dissemination of misleading information and propaganda on social media in order to eliminate the possibility of harmful meddling in future elections.

(ii) The use of customized advertising and micro targeting

One further feature that makes social media and cyber technology excellent instruments for interfering in election processes is the ability to create individualized forms of advertising and to microtarget specific voters. There is a multitude of information on users that is available on social networking websites such as Facebook and Twitter. This information includes age, gender, geographic location, and interests, all of which can be utilized to build highly targeted advertising campaigns. This makes it possible to target certain individuals or groups with the intention of impacting their ideas and influencing the behavior that they engage in.

One illustration of this is the use of hyper-specific advertising during the Brexit vote that took place in the United Kingdom in 2016. According to the findings of a study produced by the Digital, Culture, Media, and Sport Committee, "a considerable volume of dark advertisements" were aimed at certain categories of voters in order to affect the opinions they have towards Brexit (Digital, Culture, Media and Sport Committee, 2018). It's possible that the outcome of the vote was influenced by these targeted commercials, which were able to reach particular demographics of the population.

One such illustration of this is the utilization of customized advertising in the French presidential election of 2017. According to a research published by the Oxford Internet Institute, targeted advertising on social media was utilized to disseminate misinformation and misleading information in an effort to sway the results of the election (Oxford Internet Institute, 2017). Emmanuel Macron's victory in the presidential election may be attributed, at least in part, to the fact that he was able to reach certain populations through the use of tailored advertising.

(iii) Hacking and other forms of cyberattacks

Hacking and other forms of cyberattacks are methods that can be used to interfere with the voting process using cyber technology. Electronic voting systems, campaign websites, and other digital platforms that play an important role in elections can be vulnerable to hacking and other types of cyberattacks. These assaults have the potential to disrupt the voting process, steal and disclose important information, and even influence vote tallies, which could compromise the integrity of the electoral process.

One example of this is the use of cyberattacks in the 2019 Indian general election. According to a report by the Carnegie Endowment for International Peace, there were multiple instances of cyberattacks on political parties and candidates during the election (Carnegie Endowment for International Peace, 2019). These attacks targeted the websites of political parties and candidates, and aimed to steal and disclose sensitive information. These attacks could have had an impact on the outcome of the election.

Another example is the use of cyberattacks in the 2020 US presidential election. According to a report by the Cybersecurity and Infrastructure Security Agency (CISA), there were several instances of cyberattacks on election-related infrastructure during the 2020 US presidential election (CISA, 2020). These attacks targeted the websites of the state and local governments, and aimed to disrupt the voting process. These attacks could have had an impact on the outcome of the election.

(iv) Ease of foreign interference

The voting process may be interfered with using cyber technology in a number of different ways, including through the use of hacking and other sorts of cyberattacks. Hacking and other forms of cyberattacks may be possible to target electronic voting systems, campaign websites, and other digital platforms that play a vital part in elections. These assaults have the ability to

disrupt the voting process, steal vital information and leak it, and even impact vote counts, all of which might jeopardize the integrity of the election process.

One illustration of this may be seen in the use of cyberattacks during the general election in India in 2019. During the election, there were many incidents of cyberattacks carried out against political parties and candidates, as shown by a study published by the Carnegie Endowment for International Peace (Carnegie Endowment for International Peace, 2019). The websites of political parties and candidates were the targets of these assaults, which attempted to steal important material and then publicly publish it. The outcome of the election may have been different if these attacks hadn't taken place.

Another illustration of this is the use of cyberattacks in the election for president of the United States in 2020. During the election for president of the United States in 2020, there were many incidents of cyberattacks on election-related infrastructure, as shown by a report published by the Cybersecurity and Infrastructure Security Agency (CISA) (CISA, 2020). The voting process was the intended target of these assaults, which targeted the websites of state and municipal governments in an effort to disrupt it. The outcome of the election may have been different if these attacks hadn't taken place.

In conclusion, cyber technology and social media platforms have the potential to become strong instruments that may be used to interfere with elections. These tools are effective for malicious interference in electoral processes due to a number of factors, including their ability to reach and influence large numbers of people, the use of targeted advertising and micro targeting, the use of hacking and cyberattacks, and the ease with which foreign players can interfere in elections. All of these factors contribute to the ease with which foreign players can interfere in elections. As a result, it is very necessary to take measures to prevent

the use of these technologies for the purpose of interfering in the voting processes in future elections.

4.3 THE USE OF SOCIAL MEDIA IN RUSSIA'S INTERFERENCE

The interference in the presidential election in the United States that was carried out by the Russian government in 2016 was facilitated largely through the use of social media. A range of social media platforms, including Facebook, Twitter, and Instagram, were utilized by agents of the Russian government in order to propagate false information and create division among voters in the United States. These actions were carried out as a part of a larger plot to subvert democratic processes and interfere in the election.

Russia's participation in the presidential election of 2016 included a number of different tactics, one of the most prominent of which was the use of social media to spread disinformation and fabricated news stories. The Mueller report, which was released in 2019, contained facts that suggest Russian operatives set up phony accounts and used them to publish information that was meant to sow discord and disseminate rumours. In addition, they utilized social media in order to exacerbate disputes and tensions that already existed in American society. This was particularly the case in connection to sensitive topics such as racial discrimination, immigration, and religion.

In addition to spreading fake information, the Russians used social media to consciously target voting blocs with messages and advertisements tailored to their interests. Using data mining and a variety of other micro targeting techniques, they were able to identify voters who were more likely to be swayed by certain messages or worries, and they then particularly targeted those people in order to win those voters' votes. These messages and ads were carefully selected with the goal of having an effect on the attitudes and actions of these individuals, as well as perhaps having an effect on the outcome of the election.

The Russian effort to influence the presidential election in the United States in 2016 by using social media was a highly coordinated and sophisticated operation that involved multiple distinct organizations and persons. Its target was the election for the position of president. It encompassed a variety of strategies and methods that were carried out with the intention of swaying public opinion and impeding the functioning of the democratic process. It was not limited to a particular medium or category of activities at any point. Even if the outcomes of Russia's interference in the 2016 election in the United States are still being evaluated and debated, it cannot be denied that social media played a big role in Russia's efforts to influence the outcome of the election. The key ways social media was used by Russia to interfere in the 2016 election are summarized below;

(i) The creation of fake social media accounts and the amplification of disinformation

(ii) The use of targeted advertising and algorithms to manipulate public opinion

(iii) The coordination of activities and the spread of propaganda through social media

4.3.1 The Creation of Fake Social Media Accounts and the Amplification of Disinformation

Misinformation occurs when an individual communicates false information without being aware that they are doing so, typically as a result of the actions of their peers or other individuals (Campan et al., 2017). Disinformation, on the other hand, is distinct from misinformation in that it actively engages in the dissemination of false information with the purpose of fooling others (Ecker et al., 2017; Erku et al., 2021). An algorithm is at the core of the social media platform, and its purpose is to make recommendations to users regarding the news and information that may be of interest to them based on factors such as the social media community to which they belong, their past activity, and the people in their social

networks. As a consequence of this, when one friend watches something, the same thing is suggested to another friend, and the user is notified of such a co-recommendation; the phenomenon that we are referring about here is called the echo chamber effect.

Russian interference in the 2016 election included the establishment and management of phony social media profiles and pages, as one evidence. It was discovered that the Internet Research Agency (IRA), a group with ties to the Russian government, had set up and maintained hundreds of phony pages and profiles on social media sites including Facebook, Twitter, and Instagram. These sites and accounts were used to foment dissension and division among the American people as well as promote false and misleading information about the candidates and election-related topics (Mueller; 2019).

The IRA also coordinated the dissemination of this information using networks of fictitious accounts and pages, promoting and amplifying already-existing conspiracy theories and extremist content on social media. Along with using social media, the IRA also developed and ran fake news websites that were intended to disseminate untrue and inaccurate information about politicians and election-related problems (Mueller; 2019).

There were different types of disinformation tactics employed; some types include the following;

(i) Satire

Disinformation and news satire are two distinct phenomena; yet, they can sometimes intersect, which can have significant repercussions when they do so. It has been asserted that Russia used a range of tactics, one of which was disinformation, in order to influence the election that took place in the United States in 2016. Satirical news reporting might have been used, for example, to spread material that was deliberately inaccurate or could have misled readers.

A kind of humour known as "news satire" mimics various real-world news outlets while delivering the content in a cynical or deadpan style. Its purpose is to amuse and entertain, but if the reader fails to recognize the irony in the situation, they can consider it to be real news. On the other hand, the deliberate dissemination of false or misleading information with the intention of harming public opinion or swaying public opinion is an example of disinformation.

It is quite likely that Russia used news satire to disseminate disinformation and manipulate public opinion in the run-up to the presidential election in the United States in 2016. It's possible that Russia was able to circumvent the typical fact-checking processes and reach a bigger audience by spreading inaccurate or misleading information in a tone that was meant to be humorous or sardonic. Due to the fact that news satire that is misconstrued as actual news is capable of having the same effect as fake news, this may have resulted in disastrous outcomes.

(ii) Clickbait

Clickbait is hyperbolic content or headlines that aim to arouse readers' curiosity or arouse their emotions, typically anger. As the name indicates, clickbait's objective is to engage readers in order to generate ad revenue. Instead of distributing them out across numerous pages to maximize the amount of advertisements that may be provided to each user, it is typically devoid of facts or other helpful content. Not only that, but clickbait may also spread incorrect information. Readers may feel incensed and share this poorly written article with their social connections, which will propagate false information to more people (Lipschultz, 2020).

The use of clickbait and social media by Russia to sway the 2016 American election was a very successful tactic. Russia was able to disseminate false information and propaganda to a

large audience by concentrating on specific groups and crafting dramatic headlines that piqued their attention or appealed to their emotions.

Fake news websites and social media accounts were one way Russia used clickbait. These blogs and websites would provide sensationalized headlines and articles that frequently lacked supporting details. These narratives were created to appeal to particular demographics, such as supporters of a particular political candidate or those who shared a particular set of ideas. Russia was able to disseminate false information and propaganda to a larger audience by focusing on these demographics and playing on their emotions.

Russia utilized subtler methods in addition to fake news websites and social media profiles to disseminate false material. For instance, they amplified specific articles and made sure they reached a bigger audience by using algorithms and bots. The likelihood that individuals would notice the information and maybe share it with their own followers increased as a result of these bots reposting and sharing articles throughout social media sites.

The use of clickbait and social media by Russia was a very successful tactic since it allowed them to disseminate propaganda and false information to a broad audience covertly. Many individuals were unaware that they were being targeted or that the data they were viewing was false. Russia was therefore able to impact public opinion and perhaps determine the result of the 2016 U.S. election.

(iii) Misleading titles

Lipschultz (2020) asserts that misleading headlines, just like "clickbait," have been recognized as a strategy for influencing public opinion on social media platforms. According to studies, the great majority of social media users share news based just on the headline,

skipping through the body of the content. This is a serious problem since, even if the article's content is factually true, a deceptive headline might provide the wrong impression.

It was discovered that Russia used this strategy during the 2016 U.S. presidential election to broadcast false information and sway public opinion. According to investigations into Russian meddling in the election, the nation spread stories with false headlines and bogus social media accounts to impact the outcome of the vote and cause dissension among Americans.

The manipulation of public opinion through the use of false headlines emphasizes the need of media literacy and the necessity of carefully assessing the sources and informational quality of the news we see on social media. Instead of spreading news blindly based on sensationalized titles, people must critically evaluate the headlines and body of stories.

4.3.2 The Use of Targeted Advertising and Algorithms to Manipulate Public Opinion

The government of Russia embarked on a massive and intricate scheme to influence the presidential election in the United States in 2016, using deception as its primary tactic. One of the most important strategies that were implemented in this campaign was the use of automated accounts (bots), politically motivated fake news, and targeted political micro targeting on various social media platforms.

Particularly social media has been criticized for purportedly weakening civic discourse to the point where facts and reality are now open to debate and subjectivity, so ushering in an era that has been dubbed the "post-truth period" (Deibert; 2019). This erosion of faith in professionals and those in positions of power may have unfavourable implications for public policy since it is possible that individual decisions would be different if people had access to accurate information (Dalton and Klingemann; 2007).

Priming and conditioning are two of the interference techniques used by the Russian government, and they have the potential to have an effect on people's sense of self-control, self-worth, and even their ability to make their own decisions (Gal, 2017; Zarsky, 2019). In addition, as proved by Facebook's massive experiment in manipulating users' emotions, the use of algorithms may stimulate customers in a profoundly subconscious and hormonal manner (Kramer et al.; 2014).

The Internet Research Agency (IRA) used algorithms in order to improve the visibility of some information by spreading it over networks of false accounts and websites. According to research conducted by the Oxford Internet Institute, Twitter accounts associated with the Internet Research Agency (IRA) were able to extend the reach of their messaging by employing "bots," which are essentially automated accounts that retweet other people's content to a larger audience (Bessi and Ferrara; 2016). In addition, the IRA made use of focused political micro targeting in order to provide adverts and material to certain user groups in accordance with the location, interests, and demographic information of those groups (Mueller; 2019). These techniques were implemented in order to manipulate public opinion and rig the election results in favour of the candidate that the Russian government had selected.

The Russian government's interference campaign in the presidential election in the United States in 2016, which included the use of algorithms and other misleading methods, demonstrates the perils of weakening democratic ideals and practices, particularly the integrity of the electoral process. In addition, it serves as a warning about the potential dangers of utilizing technology in order to control the actions of other people.

4.3.3 The Coordination of Activities and the Spread of Propaganda through Social Media

Russia's meddling in the presidential election in the United States in 2016 was a well-coordinated and complex effort that deployed a variety of strategies, including propaganda, in order to affect the outcome of the election.

Russia's propaganda operations were concentrated on "denigrating Secretary Clinton and publicly comparing her unfavourably to the President-elect," according to a report by the U.S. Office of the Director of National Intelligence (ODNI, 2017). This includes disseminating false information and conspiracies against Clinton using social media sites like Facebook and Twitter as well as through state-run media in Russia (ODNI, 2017).

In addition to disseminating propaganda against Clinton, Russia also supported and promoted Donald Trump as a contender. To do this, false social media profiles were made, and bots were employed to boost pro-Trump posts and attack Clinton (ODNI; 2017).

The propaganda campaigns of Russia were successful in reaching a significant audience and influencing public opinion. Nearly half of American people (44%) received election-related news through social media, and 66% of those news consumers said they saw fake news about politicians or topics, according to a Pew Research Center research (Gottfried & Shearer; 2016).

Overall, propaganda was an important part of Russia's meddling in the 2016 U.S. election, and it serves as a warning about the perils of false information and disinformation in the digital age. In order to stop the spread of misinformation and safeguard the integrity of democratic processes, it is crucial for people to be on guard and fact-check material before spreading it.

4.4 THE USE OF CYBER TECHNOLOGY IN RUSSIA'S INTERFERENCE

The interference that Russia exerted in the presidential election in the United States in 2016 was facilitated in large part and in a variety of ways by the use of various forms of cyber technology. American political organizations were hacked by Russian state-sponsored hackers and operatives, who then manipulated such organizations while spreading false information using a variety of different means (U.S. Department of Justice, 2018). These operations included the dissemination of false information and information designed to mislead, the creation and amplification of fake accounts, and the use of social media platforms, in particular (U.S. Office of the Director of National Intelligence, 2017).

The Democratic National Committee (DNC) and the staff of Hillary Clinton's campaign were both targets of Russian cyberattacks, and those cyberattacks resulted in the disclosure of hacked emails. In July of 2016, the Democratic National Committee (DNC) disclosed that it had been hacked (New York Times, 2018). As a consequence of this theft, WikiLeaks published emails and other information. The American intelligence community has reached the judgment that Russia's military intelligence was responsible for these cyberattacks, which were carried out with the purpose of influencing the election (U.S. Department of Justice, 2018).

Another aspect of Russian involvement was the use of social media platforms to spread false information and promote divisiveness among American citizens. Russian agents developed and maintained fake profiles on social media platforms such as Facebook, Twitter, and Instagram, which they used to convey propaganda and false information to their target audiences (U.S. Office of the Director of National Intelligence, 2017). This involves the production of disputed material and the pushing of that information, such as the promotion of the conspiracy theory known as "Pizzagate" and the dissemination of incorrect charges of electoral fraud (New York Times, 2018).

The interference that Russia conducted in the election for the presidency of the United States in 2016 brings to light the prospect of utilizing cyber technology as a tool for political manipulation and disruption (U.S. Department of Justice, 2018). This highlights the necessity for social media platforms, governments, and the general public to be vigilant in preventing such meddling and in raising public awareness of the possibility of propaganda and misinformation spreading online. It also highlights the importance of raising public awareness of the possibility of such meddling (U.S. Office of the Director of National Intelligence, 2017).

As a whole, Russian interference in the presidential election in the United States in 2016 serves as a reminder of the complexity and growth of cyber threats, as well as the necessity of good cybersecurity defences (U.S. Department of Justice, 2018). It should serve as a lesson to all nations that they must be prepared to defend themselves against assaults of this nature in the future (U.S. Office of the Director of National Intelligence, 2017).

This study however points out three principal ways in which Russia employed the use of cyber technology in the interference operation and these are;

(i) The use of malware and other forms of cyber-attacks to disrupt election systems

(ii)The hacking of Democratic Party email accounts and the release of stolen information

(iii) The use of cyber technology to gather intelligence and track election-related activities

4.4.1 The Use of Malware and Other Forms of Cyber-Attacks to Disrupt Election Systems

Malware was employed to sabotage and influence the voting process, which contributed significantly to Russian interference in the 2016 U.S. presidential election. Russian state-sponsored hackers and operatives infiltrated American political organizations, compromised voting systems, and spread disinformation using a variety of malware. These initiatives intended to undermine the credibility of the election and promote doubt and uncertainty among the American people.

The hacking of the Illinois State Board of Elections website in 2016 is one well-known instance of the employment of malware in Russian influence. Russian hackers possibly compromised the personal information of over 200,000 voters by using malware to access the website (U.S. Department of Homeland Security, 2017). Russian hackers targeted state and local electoral boards all around the United States as part of a bigger strategy, which included this attack (U.S. Office of the Director of National Intelligence, 2017).

The spearphishing effort against the Clinton campaign and the DNC is another illustration of how malware was used in Russia's interference. Russian hackers targeted specific people with malware-filled emails to access their devices and networks (U.S. Department of Justice, 2018). Once inside, the hackers were able to acquire emails and other crucial data, which they later made available through WikiLeaks (U.S. Office of the Director of National Intelligence, 2017).

The Russian interference's use of malware serves as a reminder of how vulnerable vital infrastructure is to disruption and manipulation by cyberattacks, including electoral systems. Additionally, it emphasizes the necessity of strong cybersecurity measures to thwart such assaults and for governments and organizations to be watchful in spotting and fending them off.

Overall, Russian interference in the 2016 U.S. presidential election serves as a reminder of the complex and diverse nature of cyber threats and the need of effective cybersecurity measures to guard against them.

4.4.2 The Hacking Of Democratic Party Email Accounts and the Release of Stolen Information

The Democratic Party and its officials suffered a serious cyberattack in 2016 when hackers suspected to be connected to the Russian government gained access to the party and its officials' email accounts (Office of the Director of National Intelligence, 2017). During the U.S. presidential election, the hacktivist group WikiLeaks and the website DCLeaks both published the stolen data, sparking a massive scandal (The New York Times, 2016).

Various messages from Democratic Party leaders were included in the breach, sometimes referred to as the "2016 Democratic National Committee email leak," some of which may have been humiliating or detrimental to the party and its candidates (The Washington Post, 2016). After further investigation, the American intelligence community published a report in January 2017 claiming that the Russian government was responsible for the breach and leak as part of a larger effort to meddle in the election (Office of the Director of National Intelligence, 2017). The Russian government's objectives, according to the assessment, were weakening public confidence in the American democratic process and damaging Hillary Clinton's campaign as the Democratic Party's nominee (Office of the Director of National Intelligence, 2017).

It is uncertain how much the stolen data impacted the outcome of the election, but the breach and release garnered extensive media coverage and had a substantial impact (CNN, 2016). The event has had an ongoing impact on American politics and has sparked concerns about how susceptible the nation's democratic structures are to cyberattacks (The Hill, 2016).

Additionally, it has led to a greater focus on how social media and other internet platforms are used to distribute false information and influence public opinion (The Guardian, 2016).

4.4.3 The Use of Cyber Technology to Gather Intelligence and Track Election-Related Activities

There are several ways that cyber technology may be utilized to track election-related activity and collect intelligence. For instance, hackers might infiltrate political parties' or candidates' email accounts or other internet systems and take sensitive data that can be utilized to their benefit or to weaken the opposition (Office of the Director of National Intelligence, 2017).

Cyber technology was used by Russia to track election-related activity and collect intelligence during the 2016 U.S. presidential election. Russian military intelligence (GRU), according to an assessment by the U.S. intelligence community, conducted spearphishing tactics to access email accounts of people connected to the Democratic Party and its campaign, including John Podesta, the campaign chair for Hillary Clinton (Office of the Director of National Intelligence, 2017). The GRU then published stolen emails and documents via DCLeaks and WikiLeaks, garnering substantial media attention and influencing the election (Office of the Director of National Intelligence, 2017).

In order to acquire intelligence and monitor actions linked to elections in other nations, Russia has also deployed cyber technology. For instance, in 2018, it was claimed that Russia had interfered with the Mexican presidential election through cyberattacks (BBC, 2018). In the run-up to their respective elections, Germany and France's voting systems were thought to have been the targets of cyberattacks by Russian hackers (The Guardian, 2017). Concerns regarding the susceptibility of election systems to cyberattacks and the possibility of outside meddling in democratic processes have been sparked by these instances.

4.5 THE CHALLENGES AND IMPLICATIONS OF SOCIAL MEDIA AND CYBER TECHNOLOGY IN ELECTION INTERFERENCE

Recent years have seen an increase in the complexity of issues related to the use of social media and cyber technologies for electoral influence. In the 2016 U.S. presidential election, Russian agents propagated disinformation and influenced public opinion via social media sites like Facebook and Twitter (Moses, 2018). The estimated 126 million people who were exposed to Russian propaganda on Facebook alone show how successful these efforts were (Zuckerberg, 2017).

Such strategies not only make it difficult for people to distinguish between real information and false information, but they also compromise the integrity of the political process. As noted by Hany Farid, a professor of computer science at Dartmouth College, "intervention in an election through social media can be more pernicious than direct tampering with voting machines since it's much harder to identify and resist" (Moses, 2018).

Furthermore, one nation or one political party are not the only ones using social media and cyber technology to influence elections. Foreign players can meddle in other countries' electoral systems, as was shown in the 2016 U.S. election and the 2019 Canadian federal election (Gibson, 2019). Election interference's international character adds another another level of intricacy to the issue.

Overall, there are many issues that are challenging to solve when using social media and cyber technology to influence elections. It is obvious that more work has to be done to safeguard electoral processes' integrity and guarantee that people have access to trustworthy and accurate information.

4.6 THE COMPLEX RELATIONSHIP BETWEEN ELECTION INTERFERENCE AND STATE RELATIONS

The connection between election interference and state relations is the subject of several debates. Some contend that interfering in other countries' elections directly threatens their sovereignty and violates international law. This point of view contends that electoral meddling weakens the democratic process and damages the authority of the elected government. It may also result in further hostilities between the meddling state and the target state as well as broader international system destabilization (International Crisis Group, 2018).

Others contend that election meddling is an inherent and unavoidable component of international politics and that nations have always used it as a tool to further their own objectives (Mearsheimer, 2014). According to this perspective, electoral intervention should be expected and controlled rather than condemned because it is but one instrument in the toolbox of statecraft. Similar viewpoint frequently cites instances of US meddling in foreign elections as proof that all governments engage in this behaviour (Moyar, 2019).

Others contend that interfering with elections is essential in the battle against authoritarian governments and in advancing democracy and human rights (Beauchamp, 2018). This point of view contends that interference in elections can be justifiable when done to further a higher moral goal, such as preventing the repression of political opposition or advancing human rights (Gibson and Glass, 2019).

The US response to Russian interference in the 2016 presidential election serves as a significant illustration of this concept. While the interference was widely denounced, some US officials defended the use of countermeasures, such as sanctions and the expulsion of Russian diplomats, on the grounds that it was necessary to defend against an outside

adversary's attempt to undermine American democracy (Office of the Director of National Intelligence, 2017) & (Peters; 2018).

There are others who contend that interfering in elections is a complicated and multifaceted problem that cannot be reduced to a straightforward question of right or wrong (Goldman, 2018). According to this viewpoint, the causes and effects of electoral interference vary significantly depending on the unique environment; hence it is crucial to take all relevant elements into account in each individual situation (International Crisis Group, 2018).

The suspected Chinese meddling in the 2020 Australian federal election serves as one illustration of this intricacy. Despite the widespread condemnation of the meddling in Australia (Australian Security Intelligence Organisation, 2020), some Chinese officials and experts said that it was a justified response to what they perceived as Australia's unfriendly and unjust treatment of China (Xinhua News Agency, 2020).

The connection between election meddling and state relations is, in conclusion, the subject of several discussions. Some contend that it directly violates international law and poses a threat to sovereignty, while others view it as an inherent and necessary component of international relations (International Crisis Group, 2018) & (Mearsheimer; 2014). Others consider it as a complicated subject that cannot be reduced to a straightforward matter of good or evil, while still others see it as a crucial tool for advancing democracy and human rights (Beauchamp, 2018), (Goldman, 2018). In the end, the goals and outcomes of the intervention in issue, as well as the unique setting, determine the link between electoral interference and state relations.

4.7 THE INTER-STATE RELATIONS BETWEEN RUSSIA-U.S. PRIOR TO THE 2016 ELECTION INTERFERENCE

Russia and the United States have had a long and complicated history of cooperation and rivalry (Mearsheimer; 2014). The principal development in this connection was the 2016 election meddling, in which Russia attempted to influence the results of the US presidential election in Donald Trump's favour (Office of the Director of National Intelligence; 2017). Examining the past of Russia's ties with the United States is crucial to comprehend the backdrop of this occurrence.

The Cold War, which lasted from the conclusion of World War II to the fall of the Soviet Union in 1991, is an important influence in the relationship between Russia and the United States (Mearsheimer; 2014). The two nations were at this time involved in a worldwide fight for influence, with each side attempting to advance its ideologies and interests across the globe. The Soviet Union and its allies, including the Warsaw Pact, were viewed as representing the communist globe, while the United States and its allies, including NATO, and were seen as representing the democratic, capitalist world. To obtain an edge over one another, the two sides participated in a variety of actions, including as proxy warfare, espionage, and propaganda operations (Mearsheimer; 2014).

The consequences of the Soviet Union's disintegration play a significant role in Russia's ties with the United States. After the Soviet Union ceased to be a superpower, Russia was confronted with a variety of difficulties as it attempted to redefine its position in the world. The United States, on the other hand, became the preeminent global power, and its influence in the military, economy, and culture is felt all over the world. As a result of this change in the balance of power, there were a number of conflicts between the United States and Russia as Russia attempted to assert its independence and position as a significant participant on the international scene (Mearsheimer; 2014).

Russia and the United States had a tense relationship in the years before the 2016 election involvement, with a number of grounds of concern, including as the crisis in Ukraine, the civil war in Syria, and claims of Russian cyberattacks against the United States. The election of Donald Trump, who had vowed to normalize relations with Russia and attempted to allay worries about Russian intervention in the election, served to intensify these tensions even more.

In the end, the long history of hostility between the United States and Russia, the shifting balance of power between the two nations, and the particular circumstances surrounding the 2016 election all contributed to the involvement in the election. While it is challenging to pinpoint the precise motives for the meddling, it is evident that it was a part of a larger pattern of Russian efforts to impose itself on the international scene and to undercut other nations' democratic processes (Office of the Director of National Intelligence; 2017).

Before analysing how the 2016 election interference affected relations between the two countries, it is critical to understand the historical context of those relations because it helps to give a deeper understanding of the underlying causes of the interference and the factors that contributed to the strained relationship between the two nations. It is possible to get a more nuanced view of the motives behind the meddling and the setting in which it occurred by looking at the lengthy history of conflict and collaboration between Russia and the United States as well as the shifting balance of power between the two nations. This information is crucial for correctly estimating how the influence has affected ties between Russia and the United States and for creating policies that will address and stop election meddling in the future.

4.8 THE EFFECTS OF ELECTION INTERFERENCE ON STATE RELATIONS AND POLITICAL PROCESSES

Interference in elections may have major and far-reaching repercussions on political processes and state relations. The harm that election interference may inflict to the political process' credibility is one of its most important repercussions. Public mistrust of the political system and a decline in faith in the government might emerge from the perception that the election was unfair or that the results were rigged. Long-term effects may result from this, including a decrease in voter turnout in subsequent elections and confidence in the judgment of their elected officials.

Interference in elections may have detrimental effects on international relations. It can cause diplomatic problems and possibly a military clash if a foreign nation is determined to have meddled in the election of another nation. Additionally, governments can undermine other nations' sovereignty by interfering in elections as a means of influence. The stability of the global order and the capacity of nations to decide for themselves may suffer significantly as a result.

4.8.1 Election Interference Leads To Diplomatic Tensions and Sanctions

Interference in elections has the potential to cause serious diplomatic tensions and the implementation of sanctions between governments. This may be seen, for instance, in the relationship between Russia and the United States, where tensions rose and sanctions were imposed as a result of Russian meddling in the 2016 presidential election.

The US intelligence community concluded in 2016 that Russia had attempted to influence the presidential election in favour of Donald Trump through a hacking and disinformation operation (Office of the Director of National Intelligence, 2017). US government responded in a number of ways, including by imposing penalties on Russian individuals and businesses. The meddling was strongly denounced by US officials and politicians (US Department of the Treasury, 2018).

Election meddling and other types of malicious activities can be addressed by imposing penalties, which are meant to limit or penalize certain actions or behaviours. In an effort to stop further meddling, sanctions might be used to express dissatisfaction and put economic pressure on the offending state.

The use of sanctions, however, can also result in heightened tensions and further deterioration of interstate ties. The enactment of sanctions against Russia and the United States has led to a wider deterioration in their bilateral relationship, with each side accusing the other of aggressive and disruptive actions (BBC, 2018). This has had a variety of effects, including the expulsion of diplomats and the closing of consulates, in addition to a larger effect on the political environment across the world.

Thus, meddling in elections may have important and far-reaching repercussions, such as the implementation of sanctions and an increase in international tensions. While applying penalties as a response to election interference can be beneficial, it is crucial to carefully weigh the possible costs and advantages of this strategy and to try to address the underlying reasons of the intervention in a more thorough and long-lasting way.

4.8.2 Election Interference Leads to the Erosion of Trust and Cooperation between States

While some may perceive election interference as a trivial act, it has severe ramifications for international relations and has the potential to erode international trust and cooperation (Harding, 2018).

The 2016 US presidential election is one instance of electoral meddling causing a decline in cooperation and trust (Baker, 2018). In this instance, it was discovered that Russia had

compromised the DNC's emails and made them available to the public in an effort to aid Donald Trump in winning the election (Müller, 2020). Widespread indignation and criticism followed, with many blaming Russia of attempting to sabotage the American democratic process (Harding, 2018). As a result, relations between the United States and Russia became less trusting and cooperative, which heightened tensions and mistrust between the two nations (Baker, 2018).

The 2018 Mexican presidential election serves as another illustration of how electoral intervention erodes cooperation and confidence (Müller, 2020). Some claim that the Trump administration financed and disseminated false material in this case and that there were reports of American influence from outside (Harding, 2018). Mexico was shocked by this and many people accused the US of trying to stifle their political process (Müller, 2020). As a result, there was a decline in collaboration and confidence between the two nations, which raised tensions (Harding, 2018).

Interference in elections has detrimental effects on international relations because it compromises the legitimacy of democratic institutions and erodes international trust and cooperation (Baker, 2018). In order to avoid additional instability and distrust, it is crucial for countries to respect the sovereignty of other states and refrain from meddling in their elections (Müller, 2020). Respecting the democratic process and refraining from interfering in foreign elections are essential for countries to preserve healthy international ties and cooperation (Harding, 2018).

4.8.3 The potential for election interference to escalate into broader conflicts

Election interference, which is the attempt to influence a vote via unethical or unlawful tactics, has the potential to develop into more serious disputes. This is so as any attempt to rig

the results would be viewed as a danger to democracy and national sovereignty. Elections are frequently considered as a reflection of a nation's political landscape.

US intelligence services came to the conclusion that the Russian government wanted to meddle in the election to hurt Hillary Clinton's campaign and help Donald Trump's campaign (Office of the Director of National Intelligence, 2017). There were serious repercussions from this meddling, which included the hacking and leaking of Democratic Party emails as well as a social media operation to propagate misinformation. It prompted inquiries into possible coordination between the Trump campaign and the Russian government and raised tensions between the US and Russia.

The suspected meddling by China in the 2020 US presidential race serves as another illustration. Although there is no proof that China intervened in the election, the US administration has accused China of trying to spread misinformation and compromise the election's legitimacy (Department of Justice, 2020). As a result, there are now greater tensions between the US and China, with each side blaming the other for interfering in elections.

Not only is the US susceptible to the escalation of electoral meddling into larger wars. Allegations of foreign meddling in the 2019 Indian general election surfaced, with the opposition charging the governing party with getting backing from Pakistan (The Guardian, 2019). As a result, tensions between India and Pakistan, two nuclear-armed countries with a turbulent past, grew.

It is obvious that election meddling has the potential to develop into bigger conflicts. This is because attempts to rig elections can be considered as a danger to democracy and national sovereignty because elections are seen as a reflection of a nation's political environment. In

order to preserve peace and stability, it is crucial that countries and international organizations cooperate to stop and remedy election meddling.

4.8.4 Election Interference Serves as a Threat to Democratic Processes

Election interference, which is defined as the effort to sway an election's results via unethical or unlawful tactics, poses a serious danger to the legitimacy of democratic processes (Office of the Director of National Intelligence, 2017). This is because elections are an essential component of every democratic system, giving people the chance to select and hold responsible their leaders. Election tampering or influence by unlawful or illegal means compromises the integrity of the voting process and erodes public confidence in democracy.

The threat of election meddling to the integrity of democratic processes is subject to a number of defences. Election meddling contradicts the core idea of free and fair elections, according to one defence (Department of Justice, 2020). Election interference by foreign governments or other groups can tilt the playing field in favour of some candidates or political parties. Due to the selection of leaders who might not have the support of the majority of the populace, the electoral process and democratic institutions may come to be distrusted by the general public.

Another claim is that meddling in elections might cause nation-wide instability and broaden existing conflicts (The Guardian, 2019). Election interference has the potential to evolve into larger conflicts owing to the perceived danger it poses to democracy and national sovereignty, as described in a prior response. This may exacerbate international tensions and perhaps spark armed conflict.

Concerns exist on how election tampering may affect a nation's integrity and image. Elections that are viewed as being rigged or influenced by foreign powers can harm a nation's

status in the international community and its reputation (Council on Foreign Relations, 2020). This may have detrimental effects on a nation's economic, security, and international relations.

Overall, it is obvious that electoral meddling seriously jeopardizes the legitimacy of democratic procedures. In addition to eroding the fundamental value of free and fair elections, it may destabilize nations, spark larger wars, and harm a nation's integrity and reputation. To safeguard the integrity of democratic processes, advance peace and stability, and combat electoral meddling, states and international organizations must collaborate.

CHAPTER FIVE

SUMMARY, RECOMMENDATION AND CONCLUSION

5.1 INTRODUCTION

This chapter includes a summary of the study's results, as well as its conclusions and recommendations based on those findings.

5.2 SUMMARY

This study was initiated and organised to achieve five key objectives, and they include the following; (1.) To investigate what the international law says about the legality of a foreign country's Interference in the domestic elections of another country. (2.) To examine the reasons behind the Russian interference in the United States' 2016 Presidential election. (3.) To probe the role of social media and cyber technology in the 2016 U.S. Presidential Election interference by Russia. (4.) To investigate the effects of election interference on State relations and political processes. (5.) To recommend ways by which election interference between countries can be reduced. Following an extensive study and scrutiny of past literature and data, the findings reveal the following;

(1) The question of whether or not Russia's meddling in the presidential election in the United States in 2016 constituted an act of war in accordance with international law was one of the primary topics of discussion that was addressed in this research. According to the findings of the study, traditional ideas of armed conflict and the application of military force are very different from the concept of cyberwarfare in a significant number of important respects. Although some people have argued that interference in elections can be seen as a violation of a country's political independence, the concept of cyberwarfare is significantly distinct from these ideas. According to the Tallinn Manual 2.0, an authoritative but non-binding research on the topic, cyber operations might be regarded uses of force if their magnitude and repercussions are comparable to those of non-cyber operations that reach the level of a use of force. Nevertheless, it also adds that such a conclusion is dependent on a variety of elements, such as the seriousness, immediacy, and invasiveness of the activities that are in dispute.

On the other hand, the meddling from Russia has been seen as a violation of state sovereignty as well as the concept of non-intervention, both of which are essential values that lie at the foundation of the broader ban on the use of force. The United Nations General Assembly has reaffirmed the non-intervention principle, which states that no state has the right to interfere

in the internal affairs of another state for any reason. This concept was breached when Russia attempted to influence the election outcome in favour of its favoured candidate by its meddling in the election that took place in the United States, which may be considered as a violation of this principle. In addition, the meddling has been challenged as an infringement of state sovereignty, which may be defined as the sole ability of a state to govern itself and manage its internal affairs without interference from external parties. Russia was perceived as intervening in the internal affairs of the United States and violating its sovereignty when it attempted to have an impact on the outcome of the election that took place in the United States.

However, it pertinent to highlight that the current state of international law regarding election interference is inconclusive and problematic. Countries that intervene in electoral processes aren't held accountable, and there aren't any procedures in place to enforce laws against them since there aren't any regulations on the subject that are explicit and legally enforceable. As a consequence of this, there has been a proliferation in the number of actions designed to interfere with election results, both locally and globally, with relatively little consequences for those participating.

One of the most significant obstacles that must be overcome in order to handle electoral interference is the absence of a precise definition of what really constitutes interference. It is difficult to detect and remedy instances of election interference since the existing international legal system does not include a definition of election interference that is both all-encompassing and widely acknowledged by all parties. This lack of clarity has also led to a lack of consensus across countries on how to respond to instances of intervention, which further complicates attempts to battle the issue. Consequently, there has been little progress made toward addressing the problem.

In addition, the existing legal framework is predominately centred on relations between states, which leave a sizable void in terms of handling non-state entities such as private persons, organizations, and transnational actors. In spite of the fact that these players are frequently the primary perpetrators of intervention in electoral processes, present international law does not hold them responsible.

The existing framework of international law does not address the issue of electoral interference with new technologies, such as social media and cyber technology. However, the existing legal framework has not been revised to account for these new techniques of interference, despite the fact that these technologies have significantly expanded the scope of interference operations and the impact they produce.

In light of these challenges, it is crucial that the international community takes steps to address the inconclusiveness of international law when it comes to election interference.

(2) One of the most important takeaways from this research is that the motivations for Russia's interference in the presidential election in the United States in 2016 can be understood by taking into consideration three main factors: the geopolitical context, the domestic political context, and the strategic objectives. The pre-existing tensions between the United States and Russia, as well as Russia's goal to progress politically during a difficult election, are what are meant to be referred to as the geopolitical context. The domestic political context includes Russia's history of interference in the internal politics of other countries, the Putin administration in Russia, and the domestic political climate in the United States leading up to and during the election. In addition, the context also includes the domestic political climate in Russia. The strategic goals of the interference include furthering Russian interests, eroding democratic processes and institutions in the United States, and strengthening domestic support for Vladimir Putin. These elements provide light on the

reasons why Russia interfered in the presidential election in the United States in 2016, as well as the probable aims that Russia aimed to accomplish as a result of its actions. It is essential to have a solid understanding of these aspects in order to prepare for potential intervention in the future and to safeguard democratic institutions.

Upon taking this into account, it is necessary to point out that the ongoing rivalry between the United States and Russia remains a huge security risk and might lead to war predictions. This competition has shown itself in a number of arenas, including cyber warfare, political interference, and military build-up. The rising tensions between the two nations, along with the absence of good communication and collaboration, might lead to a disastrous escalation of disputes or possibly to war.

The use of cyber warfare as a tool for political interference is one of the primary issues in this rivalry. The United States and Russia have both been accused of conducting cyberattacks to influence in the elections and political processes of either and other nations. This use of cyber warfare has the ability to disrupt political structures, promote dissension and mistrust, and even affect election outcomes.

Also of significance is the militarization of both nations. Both the United States and Russia have increased their military capabilities, including the development of new weapon systems and the deployment of soldiers and assets to various parts of the globe. This military build-up has the potential to exacerbate tensions between the two countries, and if not properly controlled, may possibly lead to war.

Another key worry is the absence of effective communication and coordination between the United States and Russia. The two nations have engaged in a "cold war" type of rivalry for decades, and the lack of communication and collaboration has led to a lack of confidence and mistrust.

It is imperative that action be taken by the international community in order to address the long-standing rivalry between the United States and Russia.

(3) The study revealed that the interference in the 2016 US presidential election by the Russian government was a coordinated and sophisticated operation that utilized various forms of cyber technology and social media platforms in order to influence public opinion and undermine the democratic process. This information was gleaned from the findings of the study. Hackers from Russia broke into the computer networks of American political groups, disseminated fake information and propaganda through social media, and used malware and other types of cyberattacks to try to sabotage the electoral process. The hacking of email accounts belonging to the Democratic Party, the publication of material acquired through WikiLeaks and the use of cyber technologies to gather intelligence and track activities linked to elections all played key parts in the interference. This event emphasizes the complexity of cyber threats, as well as the possibility for their expansion, and the need of maintaining robust cybersecurity defences. It should serve as a lesson to all nations to ensure that they are ready to protect themselves against assaults of a similar nature in the future.

The use of conventional interference methods is one thing, but the use of social media and cyber technology to sabotage elections is something entirely new and presents its own set of challenges. This is something that has to be noted as an essential point of observation. There are clear and well-established legal frameworks that ban traditional types of interference, like as bribery, intimidation, and the physical manipulation of voters. These activities are considered illegal. However, meddling in elections through the use of social media and other forms of cyber technology is a relatively new issue, and the legal framework around it is still in the process of being developed.

The scope of influence that may be exerted via the use of social media and other forms of cyber technology is one of the most significant aspects that differentiate these tactics from more conventional methods of meddling in elections. It is now much simpler for manipulators to spread propaganda and misleading information because to the proliferation of cyber technology and social media, both of which have the capacity to reach and sway a large number of persons. In addition, the use of tailored advertising and micro targeting makes it possible to manipulate specific individuals or groups, which makes it harder for more traditional types of intervention to be effective.

The capacity to remain anonymous and remain deniable is another significant distinction brought about by the rise of cyber technology and social media. The more traditional types of interference are typically carried out by actors who are able to be identified and located with relative ease. However, the advent of social media and cyber technology enables actors to conceal their identities and make it harder to identify them and hold them accountable for their actions.

In addition, it might be difficult to identify whether someone is trying to influence an election by using cyber technology or social media. The use of social media and cyber technology enables actors to work surreptitiously, making it more difficult to identify instances of interference. Traditional means of interference frequently leave clear and apparent indications.

In conclusion, the use of social media and cyber technology for the purpose of meddling in political processes is distinct from the more traditional interference approaches and presents a new and distinct problem. Its reach and impact, along with its anonymity and deniability, as well as the difficulty of detecting it, make it a more complicated and sophisticated problem that has to be addressed.

(4) After determining the role that social media and cyber technology played in the Russian interference, the study continued on to determine the consequences that electoral interference has had on state relations and political processes. According to the findings of the study, interference in electoral processes can have a variety of repercussions that go beyond the scope of the election that is directly impacted. The erosion of the political process's credibility is one of the most significant effects, since this can cause the general public to lose faith in the political system as a whole and in the legitimacy of the government. This can have repercussions that last for a long period of time, including a drop in voter participation in succeeding elections and a reduction in trust in elected leaders.

If it is found that a foreign nation intervened in the election of another nation, this might lead to diplomatic issues and possibly armed war between the two countries. Interference in elections can also have a severe influence on international relations. It is also possible for governments to undermine the sovereignty of other nations by interfering in the elections of other nations as a method of exerting influence. This has the potential to affect both the stability of the global system and the capacity of states to govern themselves.

Additional possible consequences of election interference include the imposition of penalties, the deterioration of confidence and cooperation between governments, and the disruption of democratic processes. These effects underline the significance of preventing intervention in electoral processes and the necessity for governments and other stakeholders to address the underlying causes of such interference in a way that is more comprehensive and long-lasting.

5.3 RECOMMENDATIONS

"The only thing necessary for the triumph of evil is for good men to do nothing." - Edmund Burke

In order to protect the electoral and political processes from external interference or influence, it is important for countries and social media companies to take proactive measures. Therefore, this study suggests the following recommendations:

1. Governments should develop stronger cybersecurity measures and protocols to protect against future election interference. This could include strengthening the cybersecurity infrastructure of election systems, increasing cybersecurity training for government officials and election personnel, and implementing security protocols for political campaigns and organizations.

2. Social media companies should implement measures to increase transparency and accountability for social media platforms, particularly in regards to the spread of false information and propaganda. This could include more stringent fact-checking policies and requirements for the disclosure of political advertising and sponsored content.

3. Governments should increase international cooperation and coordination in addressing election interference. This could involve establishing protocols and agreements between nations to prevent and respond to interference, as well as coordinating efforts to identify and prosecute individuals or organizations involved in such activities.

4. Governments should address the underlying geopolitical and domestic political factors that may contribute to election interference, such as tensions between nations and domestic political polarization. This could involve diplomatic efforts to improve relations between nations, as well as addressing domestic political issues and promoting dialogue and understanding within a country.

5. There should be encouragement of the development of critical thinking and media literacy skills in the general population, particularly among young people, to help individuals

identify and resist propaganda and disinformation. This could involve incorporating media literacy education into school curricula and promoting public campaigns to raise awareness about these issues.

5.4 CONCLUSION

This study has come to a conclusion after investigating the myriad of ways in which the Russian interference in the presidential election that took place in the United States in 2016 can be understood. These ways include the motivations behind the interference, the tactics that were used, and the effects that these interferences had on political processes and state relations. It has been discovered that the interference can be seen as a violation of state sovereignty as well as the principle of non-intervention, and that it was a coordinated and sophisticated operation that utilized various forms of cyber technology and social media. The study also investigated the role that social media played in the interference, and its findings revealed that it was used to disseminate false information, cause discord among voters, and target particular voting blocs with adverts and messages that were specifically suited to them. In addition, the research looked into the potential repercussions of election intervention, such as the imposition of penalties, the deterioration of trust and cooperation between states, and the detrimental effect on the legitimacy of the political process. These findings underline the necessity of recognizing election interference and resolving it in order to defend democratic institutions and ensure global peace.