INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) AND INTER-STATE RELATIONS: THE CASE OF RUSSIA IN THE UNITED STATES 2016 ELECTION

BY

COURTNEY KORI OMORAKA
ART1510109

DEPARTMENT OF HISTORY AND INTERNATIONAL STUDIES
FACULTY OF ARTS,
UNIVERSITY OF BENIN,
BENIN CITY

DECEMBER, 2022

INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) AND INTER-STATE RELATIONS: THE CASE OF RUSSIA IN THE UNITED STATES 2016 ELECTION

BY

COURTNEY KORI OMORAKA
ART1510109

A PROJECT SUBMITTED TO THE DEPARTMENT OF HISTORY AND INTERNATIONAL STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF ARTS (B.A.) HONOURS DEGREE IN INTERNATIONAL STUDIES AND DIPLOMACY, UNIVERSITY OF BENIN, BENIN CITY

DECEMBER, 2022

CERTIFICATION

This is to certify that this work was carried out by **COURTNEY KORI OMORAKA** in the Department of History and International Studies, University of Benin, Benin City under my supervision.

COURTNEY KORI OMORAKA

_____	_____
MISS. O. OMORUYI	**FRANK IKPONMWOSA**
Project Supervisor	***Head of Department***
_____	_____
Date	**Date**

DEDICATION

This research work is dedicated to the Almighty God, for his mercies and benevolence and for preserving me against all odds.

ACKNOWLEDGEMENTS

Firstly I thank God for keeping me till this day; I will like to express my profound gratitude to my project supervisor Miss. O. OMORUYI for her contributions to the completion for my project,

I will like to express my special thanks to my honourable dad MR. Friday Omoraka and my brothers Mr destiny and Mr Gabeth Omoraka for the great love and support they have shown me all through of my studies.

Am most grateful to my Mentor, my lovely husband who has shown me nothing but love, support and words of encouragement throughout the course of my studies, thanks for looking after the kids while I studies, I love you and to my beautiful daughters Adriel, Zuri and Vandora Iyamu thanks for helping mummy..

OMORAKA KORI COURTNEY

TABLE OF CONTENTS

CHAPTER ONE

BACKGROUND TO THE STUDY

Introduction

Rapid development of information and communication technologies (ICT) has led to significant changes in social, economic and political relations of the modern society.[1] Access to information and control over it contribute to the prevalence of soft power in politics of digital age, and empower the non-state actors in international relations. Contemporary diplomatic service, besides being faced with enhanced roles, requests for extended outreach and accountability, yet shrinking resources, is also challenged with multi-stakeholder and multidisciplinary international arena.[2]

All states activities across the globe are becoming increasingly efficient as a result of globalisation and the digitization of information that have comprehensively improved the way state relate, States in the International arena are conducting their daily businesses. Studies like Laura Galante, work titled "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents"[3] argued that, ICT plays a critical role in engineering and knowledge economy as well as in management. Information and Communication (ICT) seems to assume an explanatory role in energizing the coming together of world societies. More so, it aids in the acceleration of the interdependence of institutions, organs, processes and values.[4] This study is therefore set to explore a symbiotic linkage and explain the nexus between ICT and the interstate relations as its relate to international politics. To achieve this goal, the study will examine

the historical trend of ICT in the relation to Russia acclaimed interference in the United State presidential election in 2016.[5]

In 2016, Moscow brought a threat that has long plagued many Central and Eastern European capitals to the heart of Washington, DC. Russia hacked the U.S. Democratic National Committee's system and subsequently released the confidential material to the public in a clear attempt to influence the outcome of the 2016 U.S. presidential election. The cyber-attack was paired with a disinformation campaign whose scope and reach has being assessed more than a year later. The administration of then president Barack Obama was certainly concerned about potential hacking especially given the malware attack during Ukraine's 2014 presidential election but all evidence to date suggests that the Russian government achieved significant success without actually hacking election infrastructure. The U.S. government was essentially caught off guard.[6]

It is the focus of the research work to make enquiry into important aspect of cyber-attack on the election processes. For instance the study examines how information and communications technologies are being used to undermine democratic processes. How the U.S. government was effectively caught off guard. Also examined are the challenges and threat of election democracy in the United States and the world at large.[7]

Therefore the main thrust behind the work, is, in the area elucidating the rationale behind the used ICT on the inter-states relations between Russia and United States as it relate to the cyber-attacked on the email system of the United States Democratic National Committee. The study looks into patterns on how the action alters vote tallies, vote input,

vote transmission, or other modes of counting and transmitting the voters' true choices. This does not include actions intended simply to communicate a false result or otherwise cast doubt on the reliability of the vote.[8]

It is important to examine the pattern of focus on suspected Russian government efforts, as the Russian government is widely acknowledged as the most active state in this domain. Numerous governments and independent security researchers have provided ample forensic, doctrinal, and circumstantial evidence that links interference actions to the Russian government, most prominently the Russian military's Main Intelligence Directorate (the Glavnoje Razvedyvatel'noje Upravlenije, or GRU). Nonetheless, this study makes an effort to identify specific sources and their basis for making claims of attribution to the Russian government.[9] Importantly, the study examines captures several actions commonly observed in modern cyber and information operations aimed at election interference as well as commonly documented levels of state involvement in those actions. As it relate to US 2016 elections.

Aim and Objectives of the Study

This study examines the information communications technology (ICT) and inter-State Relations: The Case of Russia in the United States 2016 Election; while the objectives include

1. To examine the evolution of ICT on international politics
2. To examine Russia and the US foreign policy posture
3. To examine the antecedence of Russia interference on the United States politics.

4. To examine what necessitated the Russian hacking of the email system of the Democratic National Committee of the United State.
5. To examine the achievement of the Russia government in hacking the Democratic National Committee email system
6. The impact and influence of the Russian hacking of the email system on the 2016 election of the United States.

Scope of the Study

The project will cover the impact of ICT on the inter-state politics with particular reference to Russia interference on the United States 2016 presidential election, from 2015 to 2018; it will also cover the affect the outcome of the United States presidential elections in 2016 and the series of investigations on the hacking of the email system of the Democratic National Committee of the United State from 2016-2018 and The study also touch on issues like ICT and its role in world politics.

Methodology

The credibility and authenticity of any research depends on the methods employed: the process of gathering, processing and analyzing data. The study will rely on data from both primary and secondary sources. The primary sources include US government gazette, publications and newspapers review from BBC and CNN and oral interviews. The secondary sources include journal, articles and extant studies of the democratic development in Nigeria. Tools like pen and paper, and camera will be used to collect information from those that will be interview after which it was transcribed for more intense analysis.

Literature Review

There are literatures on the impact of ICT on inter-state relations that the review below shows. However, there is virtually few that discusses the influence of cyber-attack on state interference on the democratic processes as it's relate to Russia cyber interference on the United States elocutionary processes. This as follow;

In Alina Polyakova work titled "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition,"[10] The article outlines the current state of play in political warfare, identifies emerging threats, and proposes potential policy responses. He argues for greater information sharing mechanisms between trans-Atlantic governments and the private sector, greater information security and transparency, and greater investments in research and development on artificial intelligence (AI) and computational propaganda.

As authoritarian regimes seek to undermine democratic institutions, Western societies must harness their current though fleeting competitive advantage in technology to prepare for the next great leap forward in political warfare. Western governments should also develop a deterrence strategy against political warfare with clearly defined consequences for specific offensive actions, while ensuring they retain their democracies' core values of openness and freedom of expression.[11]

In Laura Galante book titled Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents,[12] she posits that

> Of all the political ideas to defend themselves before the court of human history, few have proven as potent and as compelling as that of electoral democracy. Through the twentieth century, democracy has faced off many times against fascism, communism, and other ideologies, and proven itself time and again to have the stronger case. The central tenet of democracy that people should be able to select for themselves the leaders who can best govern and meet their political needs has ascended around the world, so much so that in many places it is difficult to remember that it was ever in doubt. Indeed, today's authoritarians often go to great lengths to mimic the trappings of democracy, ceding the point that elections are the best means to deliver political legitimacy.[13]

The work gave a critical detailed of Russian election interference in the United State presidential election; thus this work will be very useful in my research; especially when discussing the manifestation of the interference of the United State election.

Robert D. Blackwill, in his article "Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge,"[14] The author makes clear that the attempt by Russia to interfere with American democracy did not take place in a vacuum. To the contrary, he posits that it was and is part of a larger political and geopolitical effort designed by Russian President Vladimir Putin "to weaken the United States, divide it from its European allies, and expand Russian influence in Europe, the Middle East, Asia, and beyond." The authors are excessive in their assessment of how the current and previous American presidents and their administrations have dealt with the Russian effort to affect the U.S. election, describing their responses as "limited and ineffective."[15]

The authors advocated additional measures to better protect U.S. society, punish Russia, and deter Russia and others from continuing to directly interfere in the workings of democracies.

Jens David Ohlin in his article "Election Interference: The Real Harm and the Only Solution,[16] "asserts that although politicians and intelligence analysts have criticized Russian interference in the 2016 and 2018 elections, international lawyers seem to be at a loss for how to understand the particular harm posed by this interference. He stated that

> In addition to the hacking of email accounts and disclosure of private information, the most salient aspect of the interference was the use of social media platforms, including Twitter and Facebook, to sow division and heighten nativist tendencies within the electorate. Strictly speaking, the goal of the 2016 interference was to delegitimize a potential Clinton presidency or to help elect Donald Trump as president. But far more important was the method used to accomplish these goals: the impersonation of American citizens during participation in the political process. This latter development points to the real harm of election interference, which has less to do with sovereignty and more to do with the collective right of self-determination. Foreign interference is a violation of the membership rules for political decision-making, i.e., the idea that only members of a polity should participate in elections not only with regard to voting but also with regard to financial contributions and other forms of electoral participation.[17]

The author ended by cataloguing the mistakes of the Obama Administration in failing to expose this interference in real time which is the only way to nullify its insidious impact. Export investigations, prosecutions, and counter-measures designed to deter future misbehavior are all insufficient to nullify the impact of electoral interference. However,

recent efforts by the Justice Department and the FBI, including a new policy codified in the US Attorneys Manual, and contemporaneous indictments of Russians for interference in the 2018 election, suggest that some government actors finally understand that transparency is the only solution to election interference.

Liisa Past in his book titled "Cyberspace - Just another Domain of Election Interference,"[18] Liisa identify at first that election interference and fraud, in themselves, are not new phenomena. Neither digital nor analogue (pen and paper) technology is essentially secure or not secure per se. Rather, the specific risks of any election organization have to be assessed and mitigated case by case. She maintain that the election management bodies and legislators must find and implement solutions – digital or analogue – that technically and legally fulfill the requirements of democratic elections: free, fair and open, as well as guaranteeing a secret ballot.[19]

In as much as we agree, that these contributions and views have their own merits towards understanding what necessitated the Russian hacking of the email system of the Democratic National Committee of the United State, but we must also agree that they have not been able to give a total study of the impact and influence of the Russian hacking of the email system on the 2016 election of the United States. All the books, and articles reviewed have been able to cover only some parts of my research. Therefore, this proves to a reasonable extent that a proper study has not been carried out on the issues Russia interference on US 2016 elections with particular reference to information

computer technology. This research seeks to fill that vacuum that has been created for a long while by various scholars.

CHAPTER CHAPTERIZATION

CHAPTER ONE

BACKGROUND TO THE STUDY

The first chapter serves as a preamble to the entire work. It introduces the work and tries to give an insight of the entire body work, with its aim and objectives, the methodology used in carrying out this research, the scope of the research and various literature reviewed in relation to this study.

CHAPTER TWO

THE CONCEPT OF ICT AND IT ROLE ON INTER-STATE RELATIONS

This chapter examines the concept of ICT, the nature and structure of inter-state relations, this chapter will also highlight the various stage and activities of ICT role in inter-politics as it relate to the United State politics.

CHAPTER THREE

HISTORICAL BACKGROUND OF RUSSIA CYBER ATTACK ON U.S ELECTION

This chapter focus on the overview and antecedence of Russia interference in the United State internal politics, how it affects the conduct of the 2016 presidential election, it also examines the nature and operational mode of Cyber-attack system.

CHAPTER FOUR
THE ACHIEVEMENT AND IMPACT OF RUSSIA CYBER INTERFERENCE ON THE US ELECTION

This chapter examines the manifestations of Russia cyber interference on the US election. The chapter mainly focus on the Tenets of ICT role in the inter-state politics as its relate the Russia and the United State.

CHAPTER FIVE
CONCLUSION

This is the concluding chapter which gives a general summary of the entire research and gives possible contributions to the how Nations can prevent other state interference in their political affairs; especially as it relate to Russia Cyber-attack on the US 2016 election.

Endnotes

1. Liisa Past, "Cyberspace - Just another Domain of Election Interference," *Journal of Alternative Perspectives in the Social Sciences* Vol 1, No 1,2008, p.61.
2. Ibid.
3. Ibid.
4. Robert D. Blackwill, *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017.
5. Ibid.
6. Alina Polyakova, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition," *Journal of Religion in Africa,*Vol.42, No.5. 2017, p.333.
7. Ibid.
8. Laura Galante, "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *American Ecclesial Review*, 52, No.1, 2018, p.45,
9. Ibid.
10. Blackwill, *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017.
11. Ibid.
12. Jens David Ohlin, "Election Interference: The Real Harm and the Only Solution," *International Solidarity,* Vol.3, No.1, 2017.
13. Ibid.
14. Past, "Cyberspace - Just another Domain of Election Interference," *Journal of Alternative Perspectives in the Social Sciences* Vol 1, No 1,2008, p.61.
15. Ibid.
16. Alina Polyakova, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition," New York: Conference of New York Press, 2017, p23.
17. Liisa Past, "Cyberspace - Just another Domain of Election Interference, *"Strategic Analysis* August 2018, p.16.
18. Ibid.

CHAPTER TWO

THE CONCEPT OF ICT AND IT ROLE ON INTER-STATE RELATIONS

Introduction

This chapter looks at the relationship between Information Computer Technology and inter-State relations in the context of global politics, focusing on the relationship between the Internet and sovereign territorial states. Since inception ICT change has always had important consequences for political organization and inter-State relations.[1]International relations have always been profoundly affected by technology.[2] It is in this light that this chapter seek to survey the role of ICT on the international arena as it affect the inter-state relations.

The information revolution and the extraordinary increase in the spread of knowledge have given birth to a new era--one of knowledge and information which effects directly economic, social, cultural and political activities of all regions of the world, including Africa. Governments worldwide have recognized the role that Information and Communication Technologies could play in socio-economic development.[3]

A number of countries especially those in the developed world and some in developing countries are putting in place policies and plans designed to transform their economies into an information and knowledge economy. Countries like USA, Canada, and a number of European countries, as well as Asian countries like India, Singapore, Malaysia, South Korea, Japan, and South American countries like Brazil, Chile, and Mexico among others, and Australia and Mauritius either already have in place

comprehensive ICTs policies and plans or are at an advanced stage of implementing these programmes across their economies and societies.[4] Some of these countries see ICTs and their deployment for socio-economic development as one area where they can quickly establish global dominance and reap tremendous payoff in terms of wealth creation and generation of high quality employment.[5] On the other hand, some other countries regard the development and utilization of ICTs within their economy and society as a key component of their national vision to improve the quality of life, knowledge and international competitiveness.

Concept of Information Computer Technology

Information and Communication Technology (ICT) is a broad term concerned with technology and other aspects of managing and processing information, especially in large quantity and through some distance. To be precise, ICT deals with the use of electronic computers and computer software to store, protect process, transmit, and retrieve information. Nowadays, the term information and communication technology has taken a step to acknowledge all forms of telecommunications and processes in which messages are relayed be it through the Internet or via mobile phones. Modern telecommunication has evolved, that is not only traditional voice communications of telephones and the printed messages of telegraphs and telexes that are transmissible but television transmissions use in video conferencing in which the participants can both hear and see each other in an interactive session.[6]

Videotext is another communication service of the modern era. It consists of requesting for specific types of information over a phone and this information can be displayed on a television receiver equipped with a special decoder. It is, however, not as popular as that of data transmission epitomized by the Internet. In general the concept of telecommunication encompasses the very essence of information communication technology.[7]

The new ICT environment can be compared to "a planetary central nervous system composed of a web of communications devices, telephones, fax machines, televisions, computers, camcorders, portable digital assistants etc., all linked together into a single integrated network of digital-electronic-communications". The network never shuts down and operates at a high speed through all sorts of transmission media such as the fiber optic cables, and orbiting satellites.[8]Increasingly, it penetrates every aspect of life, from computers that operate household appliances to the cellular phones and laptop computers that provide mobile telecommunications. Perhaps most importantly, the web is an inherently interactive environment where communication flows in two directions rather than from a single source, thereby enabling instantaneous communication between anyone who is connected. These developments have had great impact on the world system and specifically on the practice of diplomacy as a component of that system.[9]

Great advancement in information technology has revolutionized the international scene and created a new communication environment. From the first geostationary satellite, Anik 1, a Canadian satellite launched in 1972, to the emergence of the internet

(formerly known as ARPANET) in 1983 and the start of the World Wide Web in 1991. It has migrated to a point where instant messaging has become the norm. The Global System for Mobile Communications (GSM) and other technologies has brought a new dimension to telecommunication and provided means to effective communication. The use of email as instant messengers and further voice and video calls over the Internet – such as Skype – has become common low-cost option for real-time communication. Mobile devices that access Internet and allow for voice, video and short messages (SMS) communications, are making the world easily and fully connected. The World-Wide Web is the most popular Internet service, is a system of interlinked information.[10]

A somewhat different but growingly populated and influential is social network – Twitter, face book, Eskimi, Skype, Viber, etc, allow for a much simpler but highly vibrant relations to be created. Users focused on broadcasting instant reflections on the world around them known as "tweets", within messages not longer than 160 characters each.[11]

The tweets are used to share personal mood, current activity or thoughts on some topic, links to online materials, interesting quotes, news or rumours. It is estimated that 27.3 million of tweets on Twitter are posted per day. Twitter-friends are commonly not friends in real life, but are rather followers of the like-minded persons and their tweets, which make the outreach of the important messages fairly global in meter of hours or even minutes. During the post-election protests in Iran in 2009 tweeting appeared to be of great help in terms of getting information out of the country and involving the huge

Iranian diaspora and those are against the regime.[12] While Twitter as the commercial platform may or may not exist in near future, the concept of tweets it developed will certainly keep its important communication role in the hectic society of today. These developments in information and communication technology have had great impact on the world system and specifically on the conduct practice of diplomacy and diplomatic services.[13]

ICT and Diplomacy

This is a different global environment in which international affairs and diplomacy has been brewing for more than forty years. The new environment that has now clearly emerged is a complex product of three broad, interrelated, and continuing revolutions, not just the information revolution. First was the end of cold war, since then the role of ideology in diplomacy has decreased. This brought some sanity to a precariously balanced arena that had the potentiality of erasing humanity off the face of Earth.[14] Subsequently, the stand-off between the Soviet Union (USSR) and the United States of America became a thing of little significance. A new political environment arose due to changes in political value. This revolution did not replace the nation-state or displace the still central role of state actors, but it did add drastically to the number of consequential entities and important players on the international scene.[15]

State actors increased in the 1960's with the emergence of newly independent colonial states of Africa and Asia and their induction into the international system as sovereigns. But it was not only the state actors that increased in size, the increasing

number of Multinational Organisation (MNO), Non–governmental Organisations (NGO), Intergovernmental Organisation (IGO) as well as Transnational Media Corporations (TMCs), has added to the complexity of international relations, thereby raised a new issue with diplomacy.[16]

The diplomatic representation of non-state actors increased and the European Union (EU) enjoys the privilege of attending economic summits such as the G-8 summit. As the number of non-state actors increase, they continue to change the nature of new diplomacy. While, intergovernmental agencies continue to prefer bilateral negotiations, MNOs begin to use multilateral meetings. The economic power of MNOs supersedes individual states and their resources and wealth are greater than the member states of the UN.[17]

The second factor is an economic revolution that has erupted, driven by the forces of liberalization, privatization, and globalization. This revolution has created an insatiable demand for information and transparency, as well as for open political processes. This revolution has also increased the number of players of concern on the global stage and change in global world-market transform the nature of diplomacy as well. Melissen and Wiseman, 1999 summarised postmodern diplomacy as a system in which both state and non-state actors can participate simultaneously. In this case, diplomat needs to be prepared to negotiate with business diplomat as a result of the increasing number and participation of business diplomats in diplomacy.[18]

Saner and Yiu, concludes that there are six new diplomatic functions of modern diplomats, the new roles are: Economic, Commercial, Corporate, business, national NGO and transnational NGO diplomacy, this express the fact that the direct effect of globalisation are clearly visible on diplomacy, as they change their roles into a business-like function. The third element is the information revolution; it is a factor that drives all the other factors. Advanced information technologies have provided new communication tools that altered existing hierarchies and power relationships among global actors.[19]Beyond these enabling effects, the information revolution and the new international environment that it fostered have made information itself a crucial source of national power and influence.

Former United state secretary of state recognises diplomatic communication as one of the important skills a diplomat should possess. Sucharipa, also emphasized the roles of diplomat in communication, but do not explain how diplomat should prepare for it. These trends have substantial impacts on diplomacy, affecting both the content and the conduct of the diplomatic enterprise necessary for successful transformation of the international arena. Furthermore, these trends offer promise of an improved security environment compared with that of the more dangerous Cold War period.[20] Even though the impacts of these three trends are largely positive, this new environment is substantially more dynamic, complex, hard to understand, and therefore challenging existence of states and the practice of diplomacy.

Contemporary Diplomacy

In recent time, diplomat now engaged in arrangements dictated by the trends in the global community: democratization, globalization, integration, information and communication technology and transnationalization. Yet, the political environment is still highly tensed with the power politics of nations, negotiations of war and peace, actualization of national interest as well as the concentration on national power and wealth. Non-state actors, with their multitude of trans-border alliances, and pressure groups have added to the traditional domain of economic diplomacy thereby partially undermining the sovereignty of states in conducting international economic relations.[21]

At the same time faced with globalization and competition for foreign direct investment as well as the growing influence of international economic standard setting organizations (WTO, ILO etc). Many countries have come to realize the global system is changing and there is need, more than ever, to redress their foreign policy objectives and project new policies to adhere to their national interests. Traditional political-military concerns, which included such issues as force balances, demarcation of territories, arms control negotiations, and alliance cohesion, have not been replaced; rather new political concerns have been added to the diplomatic menu. As a result of globalization such issues as refugees, human rights, transnational crime and terrorism, drugs, international trade, financial flows, trade, intellectual property and technology concerns, labour standards, and negotiations have now become increasingly key issues in relations between and among states.[22]

The rise of persuasive power (soft power or the ability to achieve desired outcome in the international affairs through persuasion as against coercion) is being more felt. Soft power works by convincing others to follow, or agree to norms and institutions that produce a desired conduct. Soft power can rest on the appeal of one's ideas or the ability to set the agenda in ways that shape the preferences of others. In other words, soft power recognizes that relying on traditional state-to-state diplomacy will now be less effective. Instead, people and information matter more than missiles, guns etc, indeed, there seems to be a much bigger payoff in convincing others to want what you want rather than using threats and coercion to force desired actions. Most importantly, soft power acknowledges the ICT-driven globalization.[23]

It is obvious that the information and communication technology holds the key to soft power, making it possible to appeal directly to a multitude of actors. Specifically, soft power entails that traditional diplomatic agencies tap into the wealth of knowledge of NGOs and civil society that monitor human rights, create educational exchanges and organize relief efforts. Like soft power, public diplomacy ensures to convince rather than coercion, by targeting foreign populations both the general public and opinion leaders. public diplomacy allows states to engage with key people and influence their government directly or indirectly. The potential of this subtle diplomacy is aims not at the conquest of territory or at the control of economic life, but at the conquest and control of the minds of citizens.

In other terms, public diplomacy allows a country to secure another country's consent or support by modifying the will of significant segments of its population. A Canadian specialist makes the point very clearly: "If there is initial resistance from the target government, it will be through public diplomacy that new alliances will be shaped with local groups to attempt to change policy". Public diplomacy conducted in the public space of communications technology like the Internet is one of the best guarantees for the expansion of national influences internationally.[24]

Netpolitik in International Relations

The Internet has greatly lowered the costs of transmitting information, enabling people to bypass traditional intermediaries whose power revolved around the control of information: national governments, the diplomatic corps, transnational corporations, and news organizations, among others. As a result, nongovernmental organizations (NGOs), academic experts, diasporic ethnic communities, and individuals are using the Internet to create their own global platforms and political influence. As the velocity of information increases and the types of publicly available information diversify, the very architecture of international relations is changing dramatically.[25]

These new phenomena deserve a name the word Netpolitik has been suggested to describe a new type of diplomacy that succeeds Realpolitik. Realpolitik, the German term for "power politics," is an approach to international diplomacy that is "based on strength rather than appeals to morality and world opinion."Netpolitik is a new style of diplomacy that seeks to exploit the powerful capabilities of the Internet to shape politics, culture,

values, and personal identity. But unlike Realpolitik which seeks to advance a nation's political interests through amoral coercion Netpolitik traffics in "softer" issues such as moral legitimacy, cultural identity, societal values, and public perception.[26]

Conclusion

It should be noted here that the internet and other forms of information technology, are no longer a marginal force in the conduct of world affairs, but a powerful engine for change. The internet, an electronic networking, is not only redefining work but transforming people rules, identities and social practices. Typically, the super powers govern and control the country, however, the emergence of the internet and other information technologies, enables all sorts of newcomers to enter the fray of international organizations. NGO, journalist, anti-globalization protectors, indigenous peoples and others, are finding their own voices on a global public stage.

Thus, the internet especially the usage of social media creates an alternative medium or platform for certain groups and individuals at large, to spread and pursue their agenda or propaganda.

Endnotes

1. Liisa Past, "Cyberspace - Just another Domain of Election Interference," *Journal of Alternative Perspectives in the Social Sciences* Vol 1, No 1,2008, p.61.
2. Ibid.
3. Ibid., p.62
4. Robert D. Blackwill, *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017, p.78.
5. Ibid., p.79.
6. Alina Polyakova, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition," *Journal of Religion in Africa,* Vol.42, No.5. 2017, p.333.
7. Ibid.
8. Laura Galante, "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *American Ecclesial Review*, 52, No.1, 2018, p.45,
9. Ibid.
10. Blackwill, *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017, p.53.
11. Ibid.
12. Jens David Ohlin, "Election Interference: The Real Harm and the Only Solution," *International Solidarity,* Vol.3, No.1, 2017, p.32.
13. Ibid., p.34.
14. Past, "Cyberspace - Just another Domain of Election Interference," *Journal of Alternative Perspectives in the Social Sciences* Vol 1, No 1,2008, p.61.
15. Ibid.
16. Laura Galante, "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *American Ecclesial Review*, 52, No.1, 2018, p.45,
17. Ibid.
18. Ibid., p.67.

19. Blackwill, *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017, p.34.

20. Ibid., p.35.

21. Jens David Ohlin, "Election Interference: The Real Harm and the Only Solution," *International Solidarity,* Vol.3, No.1, 2017, p.45.

22. Ibid.

23. Ibid., p.55.

24. Past, "Cyberspace - Just another Domain of Election Interference," *Journal of Alternative Perspectives in the Social Sciences* Vol 1, No 1,2008, p.61.

25. Ibid.

26. Ibid., p.62.

CHAPTER THREE
HISTORICAL BACKGROUND OF RUSSIA CYBER ATTACK ON U.S ELECTION

Introduction

The past five years have demonstrated at least one thing about election interference: though it keeps happening, nobody can agree on just what it is.[1] The 2016 US elections served as a flashpoint in recognizing modern election interference, but there have been numerous instances of interference in other European elections that can provide valuable lessons,[2] and this chapter seek to the nature and manifestations of Russia Cyber-attack on U.S election.

Manifestations of Russia Interference on US Election

The evidence that Russia interfered in the 2016 U.S. presidential election was overwhelming. As the Office of the Director of National Intelligence (ODNI) put it in January 2017 in a "high confidence "assessment based on highly classified intelligence Russia conducted an influence campaign that was "designed to undermine public faith in the U.S. democratic process, denigrate Secretary of State, Hillary Rodham Clinton, and harm her electability and potential presidency."[3]

The campaign which the intelligence community concluded was ordered by President Putin himself represented "a significant escalation in directness, level of activity, and scope of effort" of "Moscow's longstanding desire to undermine the US-led liberal democratic order "and reflected Putin and the Russian government's "clear preference for President-elect Trump."[4] According to the ODNI report and extensive

subsequent investigative reporting, Russia used a wide range of tools to achieve these goals, including the following:

Leaking Stolen Information

A major tool in the Russian intervention was to hack into the emails of private U.S. citizens and organizations and then release the stolen information in ways designed to influence the outcome of the election. Beginning at least as early as the summer of 2015 (as discovered by the FBI in September 2015), the Russian General Staff Main Intelligence Directorate (GRU) hacked the emails of the Democratic National Committee (DNC) and Clinton campaign chair John Podesta, and then used Russian or Russia-affiliated entities such as Wiki Leaks and DCLeaks to release the stolen, and income cases manipulated, data in a politically targeted manner. A day after the *Washington Post* broke the story of the DNC hack on June14, 2016, a Russia-affiliated internet persona called Guccifer 2.0 took credit for it, and on July 22 a day before the start of the Democratic National Convention Wiki Leaks published twenty thousand stolen emails, some of which included offensive comments made by leading DNC figures about Clinton's rival Bernie Sanders. The goal was to anger Sanders supporters and raise questions about the legitimacy of Clinton's nomination.[5]

Using Russian Media Outlets to Spread Disinformation

Moscow used Russian media outlets such as RT and Sputnik extensively to publish and promote false and provocative stories designed to denigrate Hillary Clinton and stoke anger among potential Trump supporters as well as Clinton's opponents on the

left. RT reportedly spent $190 million per year on programming and focused on Clinton's "leaked emails and accused her of corruption, poor physical and mental health, and ties to Islamic extremism."[6] Other areas of focus, designed to stoke controversy among Trump supporters, included fracking, the Syrian conflict, and movements such as Occupy Wall Street and Black Lives Matter. RT videos spreading allegations that the Clintons were stealing money from their own foundation or that Trump would not be "permitted" to win the election were viewed millions of times. Disinformation included in such videos was often picked up by Trump supporting media outlets such as Breit-bart News, Info wars, and Fox News' Hannity and Fox and Friends, vastly expanding their reach.[7]

Influencing Social Media Debates with Trolls and Bots

To reach more people and artificially boost perceived numbers of users on Facebook and Twitter Russia used thousands of bots (automated internet accounts) and paid internet trolls to push out disinformation to millions of Americans. According to testimony by Twitter executives in October 2017, more than thirty thousand Russia-linked accounts generated 1.4 million tweets during the final two months of the campaign. Russian Facebook pages including Being Patriotic, Secured Borders, and Blacktivist picked up controversial issues from conservative or liberal websites and promoted them to feed outrage on subjects such as race, religion, and immigration.[8] For example, when Being Patriotic posted a message rallying Americans against proposals to expand refugee settlements in the United States, it was liked, shared, or otherwise interacted with by more than 750,000 Facebook users. This Russia-promoted information, frequently

further disseminated by U.S. media outlets, often included extensive praise for President Putin and criticism of his enemies.[9]

Using Social Media Advertising

The Russian intervention also involved highly coordinated disinformation campaign of ad purchases on Facebook, Google, and YouTube. In October 2017, Facebook reported that nearly 126 million people had been exposed to content tied to Russia-linked accounts over a two-year period. Much of this advertising was paid for by the St. Petersburg-based Internet Research Agency (IRA), a secretive firm closely tied to Russian intelligence and known for spreading Russian propaganda.[10] According to Facebook, IRA likely bankrolled by the Russian oligarch and Putin ally Yevgeny Prigozh in paid $100,000 for three thousand ads to promote content on its platform, and the posts likely reached about ten million people. In buying the ads and using them for political purposes, Russia exploited a loophole in the 2002 Bipartisan Campaign Reform Act, which requires disclosure of purchasers of campaigns and forbids foreign nationals from purchasing such ads but whose definition of "electioneering communications" covers only broadcast, cable, and satellite communications not social media.[11]

Targeting Voting Systems

According to the U.S. Department of Homeland Security, Russia targeted presidential election–related voting systems in at least twenty-one states, including swing states Florida, Ohio, Pennsylvania, Virginia, and Wisconsin. Although most of these attacks were considered "preparatory activity" and most attempts to infiltrate systems

failed, two states (Arizona and Illinois) confirmed that attackers did compromise their voting systems. Investigators said that as many as thirty-nine states were targeted in attempts to manipulate and sabotage voter data.[12]

Forging Documents:

Russia allegedly produced a fake intelligence document designed to suggest collusion between the Clinton campaign and then Attorney General Loretta Lynch. Officials say that although the FBI knew the document was fake, concerns about its existence could nonetheless have contributed to the FBI Director James Comey's decision to make a highly unusual July 2016 statement harshly criticizing Clinton for her email practices even while announcing she would not be indicted.[13]

Cooperating with the Trump Campaign:

The degree of possible Russian collusion with the Trump campaign is still being investigated, but that Moscow sought at least some cooperation with numerous people affiliated with the campaign is a near certainty. As early as spring 2016 (before the U.S. intelligence community was even aware of Russian efforts), campaign foreign policy advisor George Papadopoulos was reporting to senior campaign officials that Russia had "dirt" and "thousands of Hillary Clinton's emails" and was exploring how to use them.[14]

On June 3, 2016, Trump's son and advisor Donald. Trump Jr. was offered "official documents and information" that would allegedly incriminate Clinton. A few days later, Trump Jr., campaign chairman Paul Manafort (later indicted for corruptly receiving money from a Russia-backed political party in Ukraine), and Trump senior

advisor and son-in-law Jared Kushner met in secret with Natalia Veselnitskaya, the Kremlin-affiliated lawyer who Trump Jr. had been told would deliver the incriminating information. In the weeks that followed, Trump promised to hold a news conference about Clinton's alleged wrongdoings and began to publicly praise WikiLeaks, and on July 27 called on Russia to release more Clintonemails.[15]

On July 7 and 8, Trump foreign policy advisor Carter Page traveled to Moscow, where he met with at least one senior Russian official contrary to later denials and reported to senior campaign staff that he received "incredible insights and outreach" and signals of Russia's "desire to work together."[16] On August 21, Trump advisor Roger Stone posted tweets indicating that he had advance knowledge of an upcoming leak of John Podesta's emails. And throughout October 2016, Trump Jr. had multiple online conversations with WikiLeaks about how stolen documents could be used to embarrass Clinton, some of which were followed up by tweets or comments by candidate Trump (and Trump Jr.) using the material. More important than the degree to which senior members of the Trump campaign, or Trump himself, directly colluded with the Russians is that Russia not only sought to influence the outcome of an American election but also tried to work with Americans in an effort to do so.[17]

State Involvement

State-Directed: An action that state officials, acting in their capacity as representatives of the government or government's leadership, have sanctioned and signaled their desire to achieve in some expressed manner.

State-Encouraged: An action that state officials have not directly ordered or signaled, but one in which an individual or entity with good knowledge(usually ascertained from close contact with current or former state officials) of the state's objectives can partake with reasonable assurance that these efforts will be viewed favorably.

State-Aligned: An action that individuals or entities conduct with the intention to support specific or general state objectives.[18]

Key Actors in Cyber Attacked

Advanced Persistent Threat (APT) 28:

Also known as "Fancy Bear" or "Sofacy," APT28 is a Russian government-sponsored hacking group that has been implicated in multiple high-profile cyber-attacks and intrusions since 2014 including the 2015 hack of the German *Bundestag* and the 2016 hack of US political organizations. Numerous government agencies including the US intelligence community and Department of Justice have stated that the groupAPT28 is part of the Russian military's main intelligence directorate, the GRU.[19]

Advanced Persistent ThreatAPT29:

Also known as "Cozy Bear" or "CozyDuke,"APT29 is another Russian government-sponsored hacking group that, like APT28, has been implicated in several high-profile cyber-attacks, including the 2016 intrusion into the networks of the US Democratic National Committee (DNC), the US Department of State, and the White House, and has been attributed to Russia's Federal Security Service(the *Federal'naya sluzhba bezopasnosti*, or FSB).[20]

Internet Research Agency (IRA):

Based in St. Petersburg, Russia, the IRA is an organization, often referred to as a "troll farm," that uses social media accounts to propagate frequently pro-Kremlin disinformation and amplify divisive political content. The IRA has been implicated in disinformation spread around the 2016 United Kingdom "Brexit" referendum as well as the 2016 US presidential election; notably, twelve of the thirteen Russians indicted during the Mueller investigation were employees of the IRA.[21]

Cyber Berkut: A "hacktivist" group with a pro-Russian government sentiment, active primarily in Ukraine, with the name "Berkut" referring to a professional police unit that was involved in the repression of protests during the 2014 Ukrainian Revolution. Though Cyber Berkut postures as a domestic opposition group with roots in the local Ukranian political environment, claiming to fight "neo-fascism" in Ukraine, multiple agencies including the US Defense Intelligence Agency have labeled it as a "false persona" and a "front organization for Russian state-sponsored cyber activity." Numerous security researchers, including Citizen Lab, have linked "Cyber Berkut" to APT28based on evidence such as similarities in short code and domain name formats.[22]

The U.S. Response Obama/Trump, and Congress

Considering the gravity and consequences of the Russian intervention, the U.S. response so far has been limited and ineffective. The Obama administration was slow to realize the full extent of the Russian operation, and when it did it remained reluctant to react, announcing only a limited set of retaliatory measures after the election was over.[23]

In the run-up to that election, Obama was concerned that public accusations of Russian interference would be perceived as an attempt to discredit the Trump candidacy (an accusation Trump ended up making anyway)and that retaliation could set off a mutually devastating cyber escalation with Russia which could disproportionately hurt the United States because of its greater openness and reliance on technology. These concerns led the administration to avoid retaliating in a manner proportionate to the intervention, or even from publicly highlighting the seriousness of the Russian intervention to the degree it deserved.[24]

The Obama administration did make some effort to draw attention to Russia's actions and took several steps in response. The first was an effort to win bipartisan support from Congress to jointly publicize Russia's actions, hoping that a bipartisan response would avoid the perception that the administration was acting on behalf of the Democratic candidate. However, when top administration officials sought support for a joint approach to the issue from a group of congressional leaders, presenting them with classified evidence of Russia's DNC and other cyber intrusions, they were rebuffed. Senate Majority Leader Mitch McConnell (R-KY) in particular expressed doubts about the underlying intelligence and warned that he would accuse the administration of partisanship if it publicly challenged the Russians.[25]

The Trump campaign was deeply hostile to any implication that it was receiving support from Russia, and congressional Republicans were unwilling to do anything that could help Trump's opponent, regardless of how much evidence was presented. Without

bipartisan support, and (wrongly) convinced that Clinton would win the election anyway, the Obama administration refrained from a high-profile public response.[26] The administration did proceed on its own with efforts to shore up the national voting infrastructure, but here too it faced resistance this time from state-level officials who opposed administration actions on the issue as an undue assault on states' rights.[27]

The Obama administration also took steps to warn the Russians that consequences would follow if they did not stand down. On August 4, 2016, then CIA Director John Brennan told his Russian counterpart,[28] Alexander Bortnikov, that "if you go down this road, it's going to have serious consequences not only for the bilateral relationship but for our ability to work with Russia on any issue, because it is an assault on our democracy." Obama conveyed a similar message directly to Putin in September (at a Group of Twenty summit in China), and such messages continued in numerous channels until Election Day. Some Obama officials believe this messaging deterred further Russian covert action or at least an attack on Election Day voting itself but ongoing Russian activities into 2017 suggest that its effect, if any, was limited.[29]

The administration also eventually agreed, even in the absence of bipartisan support, to make public what it knew (though the government's knowledge of Putin's role was omitted, and Obama himself did not make the statement lest it be perceived to be political). On October7, 2016, the Department of Homeland Security and the ODNI stated the U.S. intelligence community's confidence that "the Russian government directed the recent compromises of emails from U.S. persons and institutions" and that

"only Russia's senior-most officials could have authorized these activities." Designed to heighten public attention on the Russian hack, the statement was immediately overshadowed by the release of a video of Trump bragging about sexually assaulting women and, less than an hour after that, by WikiLeaks' publication of thousands of Podesta's emails. The release of the Trump tape not only drew public attention away from the intelligence community's Russia statement but also, by appearing to make a Trump victory even less likely, could have led the administration to conclude that further efforts to respond to Russia could wait until after the election.[30]

It was not until nearly two months after Trump's victory that the Obama administration actually responded to the Russian intervention. On December 29, Obama announced that the United States would expel thirty-five "intelligence operatives" and imposed new sanctions on Russian state agencies and individuals suspected in the hacks of U.S. computer systems. The new sanctions targeted the GRU (Russia's military spy agency) and the Federal Security Service (FSB, the successor to the KGB), as well as four GRU officials and three companies believed to have supported cyber operations. At the same time, Obama ordered the closure of two Russian-owned facilities on Maryland's Eastern Shore and New York's Long Island ostensibly established as recreational facilities for embassy personnel and their families but in fact used for espionage. Obama described this set of measures as "a necessary and appropriate response to efforts to harm U.S. interest," but they appear to have had little effect on Russia's ongoing activities.[31]

The Trump administration has done even less. Trump opposed Obama's December 2016 retaliatory measures, calling on "our country to move on to bigger and better things." Indeed, far from responding to Russia's intervention, Trump has refused even to acknowledge that it happened, repeatedly calling the allegations of electoral interference "hoax" and accusing Clinton supporters of making them up. During the campaign, Trump repeatedly said that he did not think it happened and (somewhat contradictorily) suggested that it could have been done by Russia but perhaps also by China or "somebody sitting on their bed that weighs four hundred pounds."[32]

In July 2017, Trump even proposed working with Russia to create a joint cyber security unit; although the unit was never created, the initiative underscored Trump's vision of Russia as a potential cyber partner rather than an adversary that had attacked the United States. And on November 11, 2017, despite the assessment of his own CIA director that Russia did interfere, as spelled out in a January 2017 joint intelligence report, Trump still claimed that report was produced by partisan "hacks" and asserted that he believed Putin's repeated denials of interference were sincere.[33]

Throughout his campaign and presidency, for reasons difficult to explain, Trump has in fact demonstrated a curious affinity for Russia in general and Putin specifically, often praising the Russian leader and rarely challenging Russian policy positions. Whereas Trump's default attitude toward virtually every other country in the world is highly critical and he insists that the United States has been getting a "bad deal," he has consistently shown sympathy and understanding for Russian perspectives and suggested

it would be "nice if we could just get along." He even relativized Putin's alleged killings of journalists and other opposition figures, asserting in a television interview that "our country does plenty of killing too."[34] During his campaign, Trump and his team softened the language on Ukraine in the Republican Party platform, expressed openness to recognizing Russia's annexation of Crimea, called the North Atlantic Treaty Organization (NATO) obsolete, questioned NATO's Article 5 commitment to collective defense, and made a priority of working with Russia in Syria.32 In November 2017, Trump was still saying he hoped to find a way to lift sanctions on Russia to promote cooperation, and insisting on Twitter that "*having a good relationship with Russia is a good thing, not a bad thing. . . . I want to solve North Korea, Syria, Ukraine, terrorism, and Russia can greatly help!*[35]

In the absence of a vigorous response by the Trump administration, it has fallen to Congress to take the lead in responding to the Russian intervention. Three congressional committees House Intelligence, Senate Select Intelligence, and Senate Judiciary are currently conducting investigations, and, despite deep partisan splits within them, all at least accept the premise that Russian intervention occurred and steps should be taken to ensure that it never happens again.[36]

Conclusion

It should be noted here that Cyberspace, and particularly election technology, has become a new domain for those who wish to suppress or interfere with the key processes of democratic societies in order to further their own ends. Based on the above analysis

one can state that US electoral democracy has once more come under challenge, threatening to undermine their hard-won social and political freedoms. Around the globe, tensions over the distribution of globalization's boons have led to widespread discontent and a resurgence in populism, while revisionist governments such as in the Kremlin have demonstrated clear intent to manipulate these seismic political forces to discredit democracy in other countries. And this will be discuss in the subsequent chapter.

Endnotes

1. Newman, L. Hay, "Officials Are Scrambling to Protect the Election from Hackers," Retrieved from URL https://www.wired.com/2016/09/electionsloom-officials-debate-protect-voting-hackers/, accessed on 12, 07, 2019.
2. Ibid.
3. Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs,* Vol.3, No.2, 2011, p.61.
4. Ibid., p.67.
5. Ibid.
6. Jordan Robertson, Michael Riley, and Andrew Willis, "How to Hack an Election," Bloomberg, March 31, 2016, https://www.bloomberg.com/features/2016-how-tohack-anelection, accessed on 23/9/2019.
7. Ibid.
8. Ibid.
9. A. Higgins, "Russians Ridicule U.S. Charge That Kremlin Meddled to Help Trump," N.Y. Times, 2017, p.34.
10. Ibid.
11. F. Howarth, "US State Department Hack Has Major Security Implications," *International Journal Affairs*, Vol.4, No.2, 2017, p.89.
12. Ibid., p.90.
13. Lior Tabansky, "Critical Infrastructure Protection Against Cyber Threats," *Military and Strategic Affairs,* p.61.
14. Ibid.
15. Higgins, "Russians Ridicule U.S. Charge That Kremlin Meddled to Help Trump,"
16. Ibid.
17. Keir Giles, *Russia's 'New' Tools for Confronting the West*, (London: Chatham House, Royal Institute of International Affairs, 2016), p.90.
18. Ibid., p.92.
19. Ibid.
20. M. Hosenball, D. Volz, J. Landay, "U.S. Formally Accuses Russian Hackers of Political Cyber Attack," p.78.

21. Ibid.

22. Kate O'Keefe and Byron Tau, "U.S. Considers Classifying Election System as 'Critical Infrastructure,'' *Wall Street Journal*, August 3, 2016.

23. James Scott and Drew Spaniel, "The Painfully Vulnerable Election System and Rampant Security Theater," ICIT Blog, Institute for Critical Infrastructure Technology, October 24, 2016.

24. Ibid.

25. Keir Giles, *Russia's 'New' Tools for Confronting the West*, (London: Chatham House, Royal Institute of International Affairs, 2016), p.90.

26. Ibid.

27. Ibid.

28. (WWW Document). Security Intelligence. URL https://securityintelligence.com/us-statedepartment-hack-has-major-securityimplications/, accessed 12th/09/2021.

29. Ibid.

30. Ibid.

31. D. Ignatius, In our New Cold War, Deterrence should come before détente, 2016. (WWW Document) Wash. Post. URL https://www.washingtonpost.com/opinions/gl obal-opinions/in-our-new-cold-wardeterrence-should-come-beforedetente/2016/11/15/051f4a84-ab79-11e6- 8b45

32. Keir Giles, *Russia's 'New' Tools for Confronting the West*, (London: Chatham House, Royal Institute of International Affairs, 2016), p.90.

33. Ibid., p.92.

34. Ibid.

35. M. Hosenball, D. Volz, J. Landay, "U.S. Formally Accuses Russian Hackers of Political Cyber Attack," p.78.

36. Ibid.

CAPTER FOUR
THE ACHIEVEMENT AND IMPACT OF RUSSIA CYBER INTERFERENCE ON THE US ELECTION

Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.[1]

Russia Cyber Attacked on US Democracy

The investigations into Russian meddling in the 2016 U.S. election continue to reveal a full-scale assault on the fundamentals of American democracy. From sophisticated social media efforts and traditional information operations to attempted hacks of voter rolls and state electoral systems, the Russians engaged in a concerted campaign to undermine American democracy and weaken trust in the democratic process and institutions.[2]

The Russians use information and influence operations and cyber tools to achieve three important and complementary goals:

- To undermine faith and confidence of democracy and its institutions from within;
- To exacerbate social and political divisions advantageous to Russian interests, including in furtherance of Russian foreign policy or simply to undermine Russia's enemies and opponents; and

- To take advantage of 21st century information environment to obfuscate or confuse the truth and amplify narratives that align with Russian interests, even when patently false.[3]

Russia's intent

These types of attacks – directed at the United States and other countries – certainly reveal the modern dangers and vulnerabilities to open, democratic processes, systems, and data. Russia is investing in concerted and sophisticated strategies to weaken competitor countries and weaken alliances, like NATO or within Europe, that are perceived to be aligned against Russian interests. As CIA Director Mike Pompeo noted in a recent address, Russian efforts to undermine American democracy have evolved and present a "serious threat."[4]

More fundamentally, they reveal a new form of combined, asymmetric influence and cyber-attacks that target democratic states and institutions. The United States and its democratic allies around the world must now treat these kinds of campaigns as fundamental, persistent, and strategic threats to the integrity of the democratic political system.[5] They must also realize that the Russian playbook can be copied and deployed by other state and non-state actors trying to influence the course of democratic societies across the globe.[6]

The details of the 2016 campaign are important and continue to be revealed as investigations in Congress and at the Federal Bureau of Investigation unfold, including

through intelligence community findings and analyses from the Department of Homeland Security. The revealed tactics expose the Russian playbook.[7]

The Russian campaign, which used state and non-state proxies, involved full-throated information operations through the use of traditional and social media, cyber hacks of political parties' emails and election-related vendors, and the probing of state electoral systems and voter rolls. As a part of this campaign, up to twenty-one state election-related networks were "potentially targeted by Russian government cyber actors," according to testimony by two Department of Homeland Security officials this summer.[8]

The recent revelations of Russian-sponsored social media campaigns through the use of Facebook and Twitter accounts and bots (automated software to facilitate internet messaging) form part of a broader campaign by Russia to affect the political discourse in the United States, to sow social divisions, and to affect the electoral process. As details emerge, the scale of the distortion has become clearer. One estimate had the number of Twitter bots at 400,000 in the months leading up to the election. Facebook has recently turned over to Congress the details of more than 3,000 ads purchased by a Kremlin-connected company.[9]

It is important to understand the elements of the threat – to be able to then devise an appropriate response and defense. There are layers to the Russian campaign in the United States, perhaps adapted or emboldened when its efforts appeared to meet little resistance or seemed to be having some effect.[10]

Though there does not seem to have been any actual cyber or other disruptions to the voting systems the day of the 2016 elections, there were attacks on state voting systems, as with the hacking of an election-service provider, and access to voting rolls, as in Illinois. The danger in such instances is the ability of foreign actors to manipulate, distort, or even destroy voting data, access, or systems.[10] This goes to the heart of the integrity of the electoral process.[11]

The Russians are taking advantage of an asymmetric information and cyber environment that allows them to operate at a distance, with relative anonymity and at low cost. The cyber tools and actors to hack emails and electoral systems are readily available, the ability to use traditional media, like *Russia Today*, to inject stories or reinforce narratives is already established, and the ability to leverage social media in an open information environment to sow discord or confusion is relatively unchecked through Facebook, Twitter, and other online and social messaging applications.[12]

Preparatory Actions

Reports of Russian activities during the U.S. election placed The Hague on high alert. It was already concerned about potential interference due to two major incidents: the alleged hacking of the Dutch Safety Board's computers in October 2015 by a group of Russian hackers known as Pawn Storm (also known as APT28 and Fancy Bear) and the alleged meddling leading up to the April 2016 Dutch referendum on a European Union (EU)–Ukraine trade deal by either Netherlands-based, pro-Russian sympathizers or activists.[13] The timing of the former incident made the objective clear: it occurred both

before and after the board published its report investigating the downing of flight MH17 in eastern Ukraine.

Despite the apparent failure, Moscow's activities had a significant impact. Local pro-Russian voices in the Netherlands actively tried to counter the hacking accusations.5 Interference leading up to the referendum was perhaps more blatant. The Kremlin was vehemently against the EU-Ukraine trade deal. A consortium of local pro-Russian, anti-Ukraine expats led by a left-wing Dutch parliamentarian, Harry van Bommel vocally opposed the deal and referred to Ukraine's pro-Western government as a "bloodthirsty kleptocracy.[14]

The opposition used in-person meetings, television, and social media to echo their views. In addition, pro-Russian agents passed themselves off as Ukrainians to infiltrate town hall meetings and Dutch groups akin to U.S. political action committees, such as the conservative Forum for Democracy, which became a major political party in 2016. During the referendum, the party repeated the Kremlin's talking points and shared Moscow's propaganda videos.8 Of course, Russian interference was not the only factor that influenced the referendum; the referendum also reflected the Dutch population's growing antipathy toward the EU. The Hague has been particularly concerned about the more amorphous threat of local populists who, knowingly or unknowingly, champion Russia's agenda in their attempts to disrupt the political status quo.[15]

The fact that the General Intelligence and Security Service (AIVD) began surveilling the Russian hacking group Cozy Bear in mid-2014 and alerted U.S. officials

to its activities in 2016 reveals just how seriously the Netherlands was taking the threat of interference. Notably, the agency was able to corroborate the U.S. Democratic National Committee hack because it was monitoring Russian activities in the aftermath of the Dutch Safety Board hack and interference in the EU-Ukraine referendum.[16]

In its 2016 annual report, the AIVD highlighted an increase in Russian influence operations targeting the country's economic, political, scientific, and defense sectors.11 The report specifically cites cyber-attacks, attempted recruitments of human intelligence, espionage, false flag operations, and the manipulation of public opinion.[17] It states that "the dissemination of disinformation and propaganda plays an important role in clandestine political influence." It also attributes an attack against 100 government email accounts to Russian activity. Dutch intelligence officers openly assert that Russians have persistently tried to "penetrate the computers of government agencies and businesses."[18]

The Dutch government took several measures to protect against potential Russian interference ahead of its March 2017 elections. Electronic voting was banned in the Netherlands in 2007 to ensure the public's trust in the democratic process, but the government felt that additional steps were necessary after receiving reports of software-related vulnerabilities. Fearing that Russia would attempt to hack into vote counting technology, it decided to ban the electronic counting of ballots and election officials' use of USB flash drives and email.[19]

The Dutch interior minister was particularly concerned about the technology's outdated software but also wanted to enhance public confidence so that "not a shadow of

doubt should hang over the results." Further contributing to the government's decision were rumors that Russia was looking to hack other elections after the 2016 U.S. election.[20] During a visit in Washington, DC, in January 2017, then Dutch foreign affairs minister Bert Koenders met with U.S. officials to discuss any specific information pertaining to potential Russian cyber-attacks against the Netherlands. While it is unclear whether any such information was exchanged, the trip is evidence of the seriousness the Dutch government ascribed to the issue of Russian meddling.[21]

In addition to the bans, the government made efforts to raise public awareness of Moscow's persistent efforts to infiltrate domestic and international governments, disrupt the political process, and influence policymaking by acquiring clandestine information through cyber espionage and human acquired intelligence. These efforts also aimed to sensitize the Dutch public to disinformation and alternative facts by highlighting and discrediting troll manufactured videos and by sharing forensic evidence that linked social media feeds by activists to Russian media outlets.[22]

Social media companies also took action ahead of the March 2017 elections. Facebook announced that it would introduce a fact-checking function to newspaper articles in the Netherlands.[23] However, in the Netherlands, mainstream media outlets continue to have a much stronger foothold than tabloids, overtly partisan news outlets, and social media companies. Consequently, there was already a significant baseline against which disinformation and alternative facts could be benchmarked.[24]

Still, the Netherlands' preparations had some shortcomings. Efforts to train politicians and government officials carried out by The Hague Security Delta and other groups generated little interest. In addition, according to information technology (IT) experts, Dutch political parties did not take sufficient steps to protect their websites prior to the elections.[25]

Notable Interference

According to the AIVD, Russia was not able to "substantially influence" the 2017 election process; its interference was mostly contained to spreading false information in the public debate.20 The Netherlands was therefore spared another high-profile incident. One reason for the limited interference might be the increased attention given to the issue by Dutch officials in recent years and the commensurate efforts to enhance preparedness such as removing electronic counting of ballots which denied Russia any opportunity to meddle.[26]

Moscow may also have been wary of further inflaming public opinion in a country where nearly 200 Dutch nationals were killed by Russian-backed rebels in the MH17 incident in Ukraine. Another reason could be that Russia values its relationship with the Netherlands, which is a major trading partner, and did not want to sow tension with Dutch leaders, especially after the MH17 incident.[27]

Potential Impact

While much of the reporting refers to the cyber element of Russian activities, the series of network intrusions, reconnaissance, and data releases appear to be tactical

weapons used in support of a broader information warfare campaign around the U.S. presidential election. Data infiltration from the networks belonging to both political parties could offer the Russian government insight to the negotiating strategies, redlines, foreign policy goals, and platforms of the incoming administration, whatever the election outcome.[28]

Cyber tools were also used to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of intelligence community reports, and prompting questions about the legitimacy of the democratic process itself. Although it is clear these operations attempted to influence American voters, the January 6 report notes that the Intelligence Community "did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election.[29]

Post-Election Responses

To further ensure the availability of reliable information during elections and referenda, Kajsa Ollongren, minister of the interior and kingdom relations, launched a dialogue with representatives of social media and technology companies to discuss the dissemination of fake news. As a result, Facebook partnered with Leiden University and a Dutch news website called Nieuwscheckers to fact-check news shared on social media. The website employs Google's fact checking feature, Google Project Shield, which, incidentally, helped protect a popular Dutch voting-information website, Kieskompas,

from a distributed denial of service (DDoS) attack during the days leading up to the March 2017 election.[30]

The government has also taken steps to strengthen Europe's collective efforts. It is considering more Dutch support for the East Strat-Com Task Force, part of the European External Action Service, and is advocating more dialogue between the EU and North Atlantic Treaty Organization (NATO) on countering disinformation.[31]

U.S. Response

On December 29, 2016, President Obama imposed sanctions for election-related malicious cyber activity by expanding an existing executive order issued in April 2015. The Obama administration identified nine individuals and entities, including Russia's two leading intelligence agencies, for election-related malicious cyber activity. Designees are subject to blocking of assets under U.S. jurisdiction, prohibitions on transactions with U.S. persons, and (for individuals) denial of entry into the United States.[32] Some have questioned whether sanctions would have a deterrent effect and if more punitive measures should be taken against the Russian government. Based on comments from U.S. officials, there may be additional responses. The nature of these activities has raised questions as to whether they constitute an act of war or espionage. There are no clear criteria for determining whether a cyber-attack should be considered a use of force that could justify a military response. Whether or not Russian cyber activity is declared an act of war, at least two authorities provide for military operations in cyberspace.[33]

Conclusions

It should be noted here that Russian interference surrounding the Dutch EU-Ukraine trade referendum, combined with the reports of Russian interference in the 2016 U.S. elections, led Dutch officials to boost their efforts to safeguard the March 2017 elections. They took significant steps to strengthen the resilience of their electoral processes and systems. That being said, Russian influence is still at work in the Netherlands, and Dutch officials need to expand their efforts to include training politicians and protecting political parties. The Forum for Democracy party now wants a referendum on remaining in the EU and is polling in second place in the Netherlands. Moreover, Geert Wilders' Freedom Party, an anti-immigration and euro skeptic party, has historically been closely aligned with Russian interests in the European Parliament and is advocating the lifting of the EU's "anti-Russian sanctions.

Endnotes

1. H. R. Clinton 'Leading by Civilian Power' Foreign Affairs 89:6 November/December 2010.
2. A.F., Cooper, Global Governance and Diplomacy: Worlds Apart? Basingstoke: Palgrave Macmillan 2008, p.118.
3. Ibid.
4. C. Edwards, 'Winning on wicked issues', The World Today, February 2008; pp 19-21.
5. Ibid.
6. Harold Nicolson, *Diplomacy*, London New York Toronto: Oxford University Press, 1963, p.17.
7. Sir Ernest Satow, *Satow's Guide to Diplomatic Practice,* London: Longman, 1979, p.7.
8. Clarence Streit, *Union Now: The Proposal for Inter-Democracy Federal Union* (London & New York: Harper & Brothers Publishers, 1940), p 22.
9. Ibid.
10. Jacob Viner, "The Implications of the Atomic Bomb for International Relations," Symposium on Atomic Energy and Its Implications," 90(1), 1946, p 56.
11. Ibid.
12. Randall L. Schweller, "The Balance of Power in World Politics," *Oxford Research Journal Affair,* Vol.2, No.1, 2001, p.56.
13. Ibid.
14. A. Higgins, "Russians Ridicule U.S. Charge That Kremlin Meddled to Help Trump," *N.Y. Times*, 2017, p.34.
15. Ibid.
16. F. Howarth, "US State Department Hack Has Major Security Implications," *International Journal Affairs*, Vol.4, No.2, 2017, p.89.
17. Ibid., p.90.
18. Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs,* p.61.
19. Ibid.
20. Higgins, "Russians Ridicule U.S. Charge That Kremlin Meddled to Help Trump,"

21. Ibid.
22. Keir Giles, *Russia's 'New' Tools for Confronting the West*, (London: Chatham House, Royal Institute of International Affairs, 2016), p.90.
23. Ibid., p.92.
24. Ibid.
25. M. Hosenball, D. Volz, J. Landay, "U.S. Formally Accuses Russian Hackers of Political Cyber Attack,"
26. Howarth, "US State Department Hack Has Major Security Implications," *International Journal Affairs*
27. Liisa Past, "Cyberspace - Just another Domain of Election Interference," *Journal of Alternative Perspectives in the Social Sciences* Vol 1, No 1,2008, p.61.
28. Ibid.
29. Ibid.
30. Robert D. Blackwill, *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017.
31. Ibid.
32. Alina Polyakova, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition," *Journal of Religion in Africa,* Vol.42, No.5. 2017, p.333.
33. Ibid.

CHAPTER FIVE
CONCLUSION

This study is aimed at finding out the impact of Russian cyber-attacks on the United State 2016 presidential election. In conclusion state-sponsored cyber-attacks are a severe, global threat. Russia's cyber-attack on the DNC demonstrated that the current international legal framework is woefully inadequate for combating this threat. The United States was forced to apply general and outdated international law principles. As a result, the United States may have violated those principles and issued a response that was ill suited for its goals: to punish Russia and deter future cyber-attacks. In the continued absence of legal reform, state-sponsored cyber-attacks will continue to occur and grow in sophistication.

In order to effectively combat against state-sponsored cyber-attacks, countries should come together and negotiate a new, international treaty specifically tailored to the issue. This treaty should contain three provisions. First, it should identify a clear and comprehensive definition of "state sponsored cyber-attack. Second, it should create an international cyber security council. Third, it should expressly authorize a punishment for state sponsored cyber-attacks. The treaty would thereby deter states from committing these attacks and provide an effective remedy when they occur.

Overall, there is growing consensus that the overarching strategic objective of Russian election interference is to undermine confidence in democratic institutions and processes generally. To achieve this goal, Russia has exploited information and

communications technology to target different dimensions of an electoral process. Based on these activities, an analytical framework begins to emerge (see figure 1). It groups the dimensions into three categories: (1) attempts to influence voters' preferences for a candidate or party, (2) attempts to manipulate the voting process itself, and (3) attempts to affect voter turnout (these are sometimes overlooked and usually aim to delegitimize the election outcome and the democratic process).

Each is tied to a different time horizon, with the first occurring over a period of months and the latter two typically occurring in a single day or over a few days. Information and cyber operations under these three categories can focus on a variety of targets, including social media platforms and conventional news organizations; the databases of political parties, campaigns, and voter registration organizations; the personal accounts of candidates or their families; and voting machines, software developers, or the transmission channels of voting results. Government actions to protect against these information and cyber operations and others include new legal measures, awareness-raising campaigns, technical changes to election infrastructure, and operational and policy changes, such as the banning of electronic vote counting. Constitutional and legal requirements in all countries limit the federal or central government's ability to implement these actions unilaterally.

A comprehensive analysis of a country's response to election interference therefore requires studying the actions of all relevant actors. Those incorporated into this framework include federal, state, and local government authorities; legislative bodies;

political parties and campaigns; election software and other relevant companies; and conventional media and social media organizations. To populate and expand the framework, further research and additional case studies should be conducted.

While research and case studies on Russian election interference are ongoing, available data point to numerous steps governments can take now to improve their preparedness. Quick action remains essential since elections will continue to be vulnerable to manipulation. Russia's decision to meddle in elections and democratic processes on both sides of the Atlantic, using cyber and disinformation tactics in particular, reflects a consistent trend that blends premeditation with opportunism. At the same time, the risk is not limited to Russian interference and must therefore be addressed regardless of the origin be it foreign or domestic. While there is heightened awareness around the issue in both the United States and European states in the aftermath of the 2016 U.S. elections, efforts to safeguard elections and protect democratic systems are still in their infancy in many countries.

It is imperative that countries launch a concerted international effort to share best practices and lessons learned: time is of the essence. Understandably, with some ad hoc exceptions, most efforts to date have been inward-focused; governments have had to quickly adjust to the new threat landscape ahead of scheduled elections. It is now urgent and crucial to begin sharing a wealth of information and knowledge before the next wave of upcoming elections. And it is a resilience-building effort that should include both advanced and struggling democracies, regardless of whether their political systems are

robust or currently under stress. Below are key governmental takeaways derived from open-source information and the European country case studies presented above. The applicability of the lessons learned herein far exceed the transatlantic relationship and can be a reference for greater international cooperation.

BIBLIOGRAPHY

Secondary Sources

Books

Blackwill, E. *Containing Russia How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, Maryknoll, NY: Orbis Books, 2017.

Cooper, A.F. *Global Governance and Diplomacy: Worlds Apart*? Basingstoke: Palgrave Macmillan 2008.

Giles, K. *Russia's 'New' Tools for Confronting the West*, London: Chatham House, Royal Institute of International Affairs, 2016.

Lev-On Azi and Cohen, E. *Connected: Politics and Technology in Israe*l Jerusalem: Israel Political Science Association, 2011.

Nicolson, H. *Diplomacy*, London New York Toronto: Oxford University Press, 1963.

Paul, T.V. Wirtz, James J. and Fortmann M. (eds.) *Balance of Power: Theory and Practice in the 21st Century*, Stanford, CA: Stanford University Press, 2004.

Satow, Ernest. *Satow's Guide to Diplomatic Practice,* London: Longman, 1979.

Streit, C. *Union Now: The Proposal for Inter-Democracy Federal Union* London & New York: Harper & Brothers Publishers, 1940.

Articles in Learn Journals

Amanah, F.H. Sheikh, S.S. "Real-Politik to Net-Politik," *International Policy Journal*, Vol.1, No1, 2015.

Clinton H.R. "Leading by Civilian Power" *Foreign Aff*airs, November/December 2010.

Edwards, C. "Winning on Wicked Issues," *The World Today*, February 2008.

Galante, L. "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents," *American Ecclesial Review*, 52, No.1, 2018.

Howarth, F. "US State Department Hack Has Major Security Implications," *International Journal Affairs*, Vol.4, No.2, 2017.

Meier, M. Lecture on "Cyber, Politics and Elections," Conference, *Yuval Ne'eman Workshop for Science, Technology and Security, Tel-Aviv University*, January 17, 2017.

Ohlin, E. "Election Interference: The Real Harm and the Only Solution," *International Solidarity,* Vol.3, No.1, 2017.

Past, L. “Cyberspace-Just another Domain of Election Interference,” *Journal of Alternative Perspectives in the Social Sciences* Vol.1, No.1, 2008.

Polyakova, Alina. “The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition,” *Journal of Religion in Africa,* Vol.42, No.5. 2017.

Schweller, Randall L. “The Balance of Power in World Politics,” *Oxford Research Journal Affair,* Vol.2, No.1, 2001.

Scott J. and Drew Spaniel D. “The Painfully Vulnerable Election System and Rampant Security Theater,” *ICIT Blog, Institute for Critical Infrastructure Technology*, October 24, 2017.

Tabansky, L. “Critical Infrastructure Protection against Cyber Threats,” *Military and Strategic Affairs,* 2017.

Viner, J. “The Implications of the Atomic Bomb for International Relations,” *Symposium on Atomic Energy and Its Implications*,” 90(1), 1946.

Magazine

Higgins, A. “Russians Ridicule U.S. Charge That Kremlin Meddled to Help Trump,” *N.Y. Times*, 2017.

Internet Materials

Newman, L. H. “Officials Are Scrambling to Protect the Election from Hackers,” Retrieved fromURLhttps://www.wired.com/2016/09/electionsloom-officials-debate-protect-voting-hackers/, accessed on 12, 07, 2019.

Robertson, J. Michael Riley, and Andrew Willis, “How to Hack an Election,” Bloomberg, March 31, 2016, https://www.bloomberg.com/features/2016-how-tohack-an election, accessed on 23/9/2019.

Security Intelligence. URL https://securityintelligence.com/us-statedepartment-hack-has-major- security implications/ (accessed 11.1.16).