2018

Are Cyber Operations Having an Impact on State Electoral Processes?

Sean Joseph McNicholas

CUNY City College

How does access to this work benefit you? Let us know!

Follow this and additional works at: https://academicworks.cuny.edu/cc_etds_theses

Part of the Political Science Commons, and the Soviet and Post-Soviet Studies Commons

Recommended Citation

https://academicworks.cuny.edu/cc_etds_theses/748

This Thesis is brought to you for free and open access by the City College of New York at CUNY Academic Works. It has been accepted for inclusion in Dissertations and Theses by an authorized administrator of CUNY Academic Works. For more information, please contact AcademicWorks@cuny.edu.
Are Cyber Operations Having an Impact on State Electoral Processes?

Sean McNicholas

May 2018

Master’s Thesis
Submitted in Partial Fulfillment of the Requirements for the Degree of Master of International Affairs at the City College of New York

COLIN POWELL SCHOOL FOR CIVIC AND GLOBAL LEADERSHIP

Advisor: Professor Jean Krasno
Second Advisor: Professor Bruce Cronin
# Table of Contents

Abstract: .......................................................... 3

Chapter One: Introduction: ........................................... 4

Chapter Two: Literature Review: ....................................... 7

Chapter Three: Overcoming Definitional Fog: ....................... 17

Chapter Four: Types of Cyber Operations: .......................... 29

Chapter Five: Purposes behind the Cyber Operations: ............... 48

Chapter Six: Quantifying the Effects: .................................. 62

Chapter Seven: Russia’s International Meddling and Active Measures – An Interview with a Former Eastern European Official: ................................. 75

Chapter Eight: Conclusions and Recommendations: .................. 88

Bibliography: .......................................................... 100

Annex A: ............................................................. 111

Annex B: ............................................................. 121
Abstract

Cyber-attacks have become common occurrences which have an impact on all aspects of life ranging from business transactions to personal communications. Alarmingly, coordinated cyber-attacks are increasingly targeting politicians and their associates, political campaigns, political organizations and the broader public with political messaging. Given the novelty of these new forms of attacks, little is known of their potential impact. This thesis argues that states, state-directed actors, or non-state actors are disrupting, altering or influencing the electoral process in democratic states through coordinated cyber operations. It further argues that the purpose is to increase hyper-partisanship and erode the legitimacy of democratically-elected leaders.

A quantitative study analyzing the data from a test group of consolidated democracies which had experienced these types of cyber operations displayed declining confidence in both their national governments and the honesty of their elections. By investigating the most prominent and verifiable cyber-attacks against state election processes, a connection between the attacks and Russia’s state intelligence services became apparent. Further research revealed Russian intelligence agencies’ historic use of covert ‘active measures’ and their current efforts to incorporate cyber operations within those measures, thus increasing active measures’ versatility and efficiency. Historic and geopolitical insight provided by an ex-official from a former Soviet Republic contextualized how these new cyber operations could be used to advance Russian geopolitical objectives.
Chapter One: Introduction

Many national security experts and academics are deeply concerned over the threat posed by cyber operations. While various forms of cyber operations have become common, the alleged use of coordinated cyber operations to affect national elections in democratic countries is a new type of occurrence. As a result, there has been little in the way of academic research conducted on this new type of vulnerability. Given the limited breadth of research material, this thesis will examine public survey data collected from states which have allegedly been the victims of a coordinated cyber operations targeting national elections with the goal of directing electoral outcomes. Coordinated cyber operations appear to have been designed to manipulate a population’s perceptions of elected leaders’ legitimacy and partisanship in their national political debates.

The issue of electoral interference in democratic states through the use of coordinated cyber operations is of critical importance. Attempts to interfere in states’ electoral processes, whether or not they are successful, undermine the legitimacy of the electoral process which is the bedrock of a functioning democratic state. If the outcome of an electoral process is called into question, there will be an erosion of the legitimacy that the electoral process bestows on democratically elected leaders. In addition, foreign states may gain undue influence in electing leaders who favor the foreign state’s policy positions. This erosion of legitimacy may lead to increased hyper-partisanship and can sow doubts among the national electorate regarding the policy decisions of any elected leader.
In researching this thesis, I aim to answer and provide insight into the following questions:

- What is the evidence that there have been verifiable attempts by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?
- What were the methods used by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?
- What were the effects of attempts by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?

I argue here that states, state-directed actors, or non-state actors are disrupting, altering or influencing the electoral process in democratic states through coordinated cyber operations. I further argue that the purpose is to increase hyper-partisanship and erode the legitimacy of democratically-elected leaders. This can also lead to undue influence and promote candidates that support a foreign state’s preferred policy positions. Russian influence in Eastern Europe is a prime example.

This thesis will rely heavily on quantitative data from global surveys that track voter’s perceptions of elected leader’s legitimacy and their views of national partisanship politics in democratic countries. The thesis compares the voter’s perceptions of elected leader’s legitimacy and their views of national partisanship politics, comparing results taken prior to alleged cyber operations designed to interfere in elections with perceptions after such allegations. It will also compare the data from democratic countries in which
there have been allegations of cyber operations used to conduct electoral interference with a control group of democracies. Qualitative analyses will be undertaken to explain the data’s results. Furthermore, qualitative sources will be used to supplement the quantitative survey data where possible.
Chapter Two: Literature Review

This chapter reviews the existing literature surrounding cyber operations and how states are responding to the new challenges and opportunities they present. It also provides an overview which places cyber operations within the broader context of international relations and international humanitarian law. Further, this chapter addresses the surveys used to explain their significance in this paper’s findings. While chapter three provides specific definitions for various disputed terms such as ‘cyber-attack’ and ‘cyber operation’ as they will be used in this paper, the language utilized here reflects that of the experts and scholars being cited.

Discussions around cyber-attacks and cybersecurity have become increasingly common in a range of different forums including academic research, national security debates, in the media and in corporate and nonprofit organizations’ guidelines. Yet, in this nascent field there is little consensus on precise terminology. Ambiguous terms like ‘cyber-attacks’ can be used to describe attacks ranging from state-sponsored, enduring sophisticated and multipronged campaigns against rival states to attacks in which one rogue actor gaining unauthorized access to a private citizen’s email account. Considering the disparity, it is important to begin with a compilation of existing definitions for cybersecurity and information security. In 2014, Robert Morgus and Tim Maurer compiled definitions as they are utilized by various governments, international organizations and research institutes. To illustrate this diversity, there are forty-seven

different entries for ‘cyber security’ offered by a variety of states, agencies and organizations often embracing multiple definitions.

**Cyber Policy and Practice**

For those unversed in cybersecurity issues, Peter Singer and Allan Friedman’s work *Cybersecurity and Cyberwar: What Everyone Needs to Know* offers a comprehensive overview of cybersecurity and many of its associated issues, including: a basic overview of cyberspace and security, categorization of types of cyberattacks, cybercrime, cyber espionage, cyberterrorism, cyberpiracy, the intersection of cyber issues and foreign policy as well as the institutions and bodies that govern cyberspace.² Equally noteworthy, in 2013 the United Nations Institute for Disarmament Research (UNIDIR) released its *Cyber Index* which offers a useful and comprehensive guide to state civilian policy positions and state military doctrines as well as international and regional organization’s positions on cyber security.³

In *Defending a New Domain: The Pentagon’s Cyberstrategy*, William Lynn, a former U.S. Deputy Secretary of Defense situates all the potential and theoretical cybersecurity threats in everyday practice. The emergence of cyber warfare has created an asymmetrical imbalance in which a relatively small number of determined actors can identify and exploit vulnerabilities in an adversary’s cyber infrastructures with a relatively low cost and risk.⁴ Further escalating this threat is the multitude of potential

---

targets which can include: national security agencies, governmental agencies, financial institutions, commercial operations, transportation networks, critical infrastructure and power utilities. The potential impact of such cyber-attacks could range from the slow erosion of U.S. military preparedness and its global economic competitiveness to the massive loss of life and property. The article also outlines the Pentagon’s efforts to respond to these challenges with the creation of the U.S. Cyber Command in 2010 which consolidated the cyber operations of the various branches of the military under one unified operation. The Cyber Command was tasked with the security of all defense and military operations in cyberspace, coordinating the use of the resources dedicated to cyber defense and building partnerships with the U.S. intelligence agencies. Beyond greater internal coordination, the Pentagon is also leveraging the U.S. tech industries’ expertise to identify and address vulnerabilities in civilian cyber infrastructure.

**International Law and Cyber Norms**

The most thorough and up-to-date examination of international law in relation to cyber security was produced in 2017 by the NATO Cooperative Cyber Defence Centre of Excellence in a follow up edition titled the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. The manual builds off the first edition which was released in 2013 and identifies 154 well-established legal rules as they apply to governing cyber operations. Reflecting the fact that cyber operations are becoming an increasingly common tool used by states, the first version focused on the evolving use of the most severe cyber operations which could invoke the use of force and right to self-defense.

---


6 Ibid.
The second edition prioritizes a legal analysis for less severe, day-to-day cyber operations and lays out a more comprehensive view of the various international and regional bodies that govern and deliberate on cyberspace. Michael Schmitt, the renowned cyber scholar and lead editor on the *Tallinn Manual* projects also contributed to the classification of cyber conflicts. In the 2013 article, *Classification of Cyber Conflict*, Schmitt uses the guidelines laid out in the Geneva Conventions to analyze and illustrate the different classifications using the 2008 international armed conflict between Georgia and Russia as a case study. This article’s most significant contribution was outlining the factors that elevate the significance of a cyber conflict and specifying the appropriate countermeasures the defending nation could employ.

In *Constructing Norms for Global Cybersecurity* Martha Finnemore and Duncan Hollis argue that despite the novelty of the cyber realm, many of factors that are critical in the norm development process remain the same. They emphasize that norms already exist in the form of national regulations, international laws and professional standards and that no one set of ‘norms’ could address the wide array of issues which affect such a diverse community. They argue that only a pluralistic, multi-stakeholder form of governance could work on a platform as diffused as the internet. By using a mixture of incentives, persuasion and socialization methods they assert that norms can be developed and change online habits. By applying the rich social science literature on norm

---


construction, Finnemore and Hollis tend not to see norms as an end product, but rather as a process and a support more for participants and different forums in the dialog surrounding the governance of the cyber realm.

A 2017 publication by UNIDIR, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, outlines international organization’s efforts in the normative process surrounding state behavior towards Information and Communication Technologies (ICTs).\(^{10}\) While primarily addressing the work of the General Assembly and the UN Group of Governmental Experts (GGE), the publication also looked at the role of regional organizations and confidence building measures to ensure stability of the ICT environment and highlighting where on-going sources of disagreement exist.

Given the range of international issues and disagreements that stem from cybersecurity, many experts in the field have advocated for a cyber treaty convention. One leading scholar, Rex Hughes, a fellow for cyber security at Cambridge University, wrote *A Treaty for Cyber Space* in 2010 to address these specific concerns.\(^{11}\) Hughes’ piece, surveying several military officials and cyber security experts, asserts that the next major interstate conflict is likely to begin in the cyber realm as long as there are no established expectations of cyber conduct nor mechanisms to deescalate a cyber conflict.\(^{12}\) The article puts forward the aspects Hughes sees as necessary for an enduring

---

12 Ibid.
cyber treaty, while many are based on the Law of Armed Conflict, they are adapted to the
cyber realm and emphasize: only targeting infrastructure with military capabilities, strict
distinctions between military and civilian targets, nonuse of indiscriminate weapons and
respect for the principles of perfidy, neutrality and proportionality.\(^\text{13}\)

In Cameron Brown and David Friedman’s 2014 article, entitled *A Cyber Warfare
Convention? Lessons from the Conventions on Chemical and Biological Weapons*, the
concept of a cyber treaty convention is also supported while applying additional insight
from previously successful conventions.\(^\text{14}\) While the authors, experts in the field of arms
control, concede that it is impossible to know how many states abandoned attempts to
acquire biological or chemical weapons as a result of these conventions, they point to
statistical evidence that supports their claims that the conventions had an overall impact
on declining proliferation numbers. They also address several issues first acknowledged
in the chemical and biological conventions that they believe would be applicable to a
cyber convention today, such as: independent verification and enforcement regimes,
monitoring of “dual use” technologies, and defining the scope of what is to be covered
under the convention.\(^\text{15}\) The article also outlines various shortcomings of the previous
conventions such as the role of non-state actors, which would benefit a cyber
convention.\(^\text{16}\)

https://citizenlab.ca/cybernorms2011/treaty.PDF.

\(^{14}\) Brown, Cameron S., and David Friedman. “A Cyber Warfare Convention? Lessons from the
Conventions on Chemical and Biological Weapons.” *Arms Control and National Security: New Horizons.*

\(^{15}\) Ibid.

\(^{16}\) Ibid.
Informational Warfare and Cyber Aggression

While this thesis seeks to uncover any and all alleged attempts to disrupt, alter or influence the electoral process in democratic states through coordinated cyber campaigns, Russian prolific and aggressive use of these new tactics has earned it the greatest scrutiny from rival militaries, intelligence agencies, and governments as well as cyber experts and increasingly academics. The most comprehensive overview of how Russia has been utilizing cyberwarfare to further its foreign policy agenda was produced by the U.S. Senate Committee on Foreign Relations in January, 2018. The report, Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security, offers a detailed examination of how Russian President Vladimir Putin ascended to power and how he adapted Soviet-era KGB techniques such as ‘active measures’ and ‘malign influence operations’ to the modern era. In the process, he turned Moscow’s Federal Security Services (FSB) into an extremely effective intelligence agency. According to the report, Putin used techniques such as staging disinformation campaigns against adversaries, cultivating political extremist groups, and weaponizing both information and energy supplies all with the goal of gaining leverage over adversaries. Once Putin had perfected these methods on his domestic opposition, he began to employ them abroad to advance his foreign policy goals. The report builds an in-depth chronology tracking these Russian attempts to disrupt and manipulate international rivals from Russia’s near abroad, in the Caucasus and Eastern Europe, to its attempts in Western Europe and the

---

18 Ibid.
The report concludes with expert analysis on the methods of attack which proved most effective and recommendations on how such efforts can be undermined when Russia attempts to use them again.20

Yet, the U.S. is not alone in recognizing this new threat. In fact, many European nations have suffered such attacks and have been attempting to address the problem for months and years. The use of what many experts are calling “hybrid warfare” – a mixture of conventional warfare supported by cyber aggression and disinformation campaigns - in Russia’s assault on eastern Ukraine and annexation of Crimea served as a wakeup call for European militaries and intelligence agencies.21 In a NATO report, The Next Phase of Russian Information Warfare, Keir Giles, a leading Russian scholar at Chatham House, analyzes how Russia will likely work to further integrate its cyber capabilities with its conventional arms to devastating effect. Giles also outlines what NATO members are doing to mitigate the effects and offers recommendations to help further those efforts.22

Polling Surveys & Data Collected

One of the primary data sources used in this thesis comes from Gallup Inc. in the form of their annual World Poll and the U.S. Daily surveys. Gallup’s methodology aims to collect data representative of the civilian population ages 15 and older by conducting approximately 1,000 interviews in the respondent’s native language. With over 150

---


20 Ibid.


22 Ibid.
countries included in the survey, Gallup conducts its interviews by phone in countries where telephone coverage extends to at least 80% of the population while conducting face-to-face interviews to maintain accurate national representation in countries which this standard is not met. Interview questions range in topic but inquire about the respondent’s view of minorities and immigrants, freedom of the media, internet access, economic conditions, global leaders, national leaders, corruption in business, corruption in institutions, corruption in elected leaders as well as election integrity. The data collected for this paper includes worldwide national aggregates for this data from 2006 to 2017 as well as national data broken down by annual income, educational attainment, age and the urban-rural divide for nations hailing from NATO, the former-USSR and any European nation not included in the former categories. The same polling data was also collected on a sub-national, state-by-state basis in the United States.

Another crucial source of information collected for this thesis comes from Edelman, a consultancy firm which has produced the annual Edelman Trust Barometer since 2001. Edelman’s methodology includes collecting polling data from 28 countries via online surveys. Their data is broken into two categories: the ‘Mass Population’ which is collected from 1,150 respondents (ages 18 years and older) per country which represents 85% of those polled and an ‘Informed Public’ which is collected from at least 200 respondents per country and represents 15% of those polled. In addition, the ‘Informed Public’ must meet four criteria including: those who fall within the age range of 25 – 64, be college-educated, represent the top 25% of household income per age

group in each country and report significant media consumption and engagement in business news and public policy. The data is collected from more than 33,000 respondents globally and fields questions about a respondent’s trust in institutions including: specific industries and sectors of the economy as well as the business community at large, the media, NGOs and national governments. Furthermore, the survey asks additional questions for each institution in an attempt to understand the factors that have an impact on the population’s trust in a specific institution.

The final survey included here comes from the Pew Research Center which has produced its annual Global Attitudes Survey in 91 countries since 2014. Pew’s methodology employs both face-to-face (when necessary to attain a representative national survey) and phone interviews in the native language with an average of 1,000 respondents per country. While the Global Attitudes Survey asks many questions regarding the respondent’s economic outlook and view on global trends, it also offers insight on a respondent’s attitudes towards global organizations and institutions, various world leaders and the countries they represent.

Building a Comprehensive View

Together these sources help to build a more complete picture of the threat posed by cyber aggression and help illustrate the effects it has on government and their citizens.

This thesis contributes to the debate by adding structure to the opaque field of cyber

---

26 Ibid.
28 Ibid.
aggression and defense. It brings clarity by indexing the different methods and tactics that have been used against democratic states’ governments, political parties, individual political actors, electorates at large and of course their electoral processes. Separately, the sources provide alarming but disparate aspects of the threat from cyber aggression. Yet when viewed comprehensively as different aspects of a multipronged assault on democratic institutions globally, they establish an urgent need for a collective and proactive response from all those who value democratic governance.
Chapter Three: Overcoming Definitional Fog

In order to properly situate this thesis within the wider conversation surrounding cybersecurity, it is necessary to establish definitions and clarify concepts as they are to be used within this context. For organizational purposes, the definitions and concepts will be broken into two categories: intelligence operations and cyber aggression and security. This distinction will help to show how many of the modern techniques for cyber aggression and defense have been adapted as yet another set of tools, albeit very effective tools, used within the larger context of intelligence operations. For terms or concepts that have multiple definitions, this thesis uses the most applicable or widespread usage.

Intelligence Operations

One of the keys to understanding how states, and in particular Russia, have taken advantage of cyberspace requires an understanding of the intelligence agencies which have been making use of the new technologies. The so-called Gerasimov Doctrine and the concept of ‘hybrid warfare’ both explain why Russia and others following Russia’s lead have embraced cyber technology so thoroughly.29 Andrew Monaghan writing for the US Army War College in 2016 provided a definition for hybrid warfare which outlines the concept in great detail. Hybrid warfare exists “between war and peace” and makes use of “Russian asymmetric challenges such as economic manipulation, an extensive and powerful disinformation and propaganda campaign, the fostering of civil disobedience and even insurrection and the use of well-supplied paramilitaries. In sum, Russian hybrid

warfare as widely understood in the West represents a method of operating that relies on proxies and surrogates to prevent attribution and intent, and to maximize confusion and uncertainty. Conventional force is often obliquely mentioned as a supplementary feature, but the main feature of hybrid warfare is that it remains below the threshold of the clear use of armed force. Hybrid warfare is thus tantamount to a range of hostile actions of which “military force is only a small part, or ‘measures short of war’ that seek to deceive, undermine, subvert, influence and destabilize societies, to coerce or replace sovereign governments and to disrupt or alter an existing regional order.”

This definition of hybrid warfare is the essence of the Gerasimov Doctrine, a phrase first used in an article published in *Voenno-promyshlennyi kur’er*, the *Military-Industrial Courier* in 2014 by Russian Chief of the General Staff Valery Gerasimov and illustrates how deeply this concept is embedded within the Russian leadership. However, as some scholars have found issues with attributing the doctrine to Gerasimov and even that it constitutes a doctrine, this thesis will mark use of Monaghan’s widely accepted definition of hybrid warfare.

Within Monaghan’s definition of hybrid warfare, he describes the use of asymmetric challenges to deceive, undermine, subvert, influence and destabilize societies, to coerce or replace sovereign governments and to disrupt or alter an existing regional order. Monaghan is describing what Russian and Soviet intelligence officers called *Aktivinyye meropriatia*, or active measures. Writing extensively on the history of

---

32 Ibid.
the Soviet Union and its intelligence services, the Komitet Gosudarstvennoy Bezopasnosti (KGB), Christopher Andrew and Vasili Mitrokhin describe active measures developing alongside the agency which was established in 1954. Andrew and Mitrokhin leave the definition as broad as possible, considering the malleable nature of active measures, defining them as Soviet efforts “to influence the course of world events” with operations ranging from media manipulation to various degrees of violence. While the thesis will use this broader definition, more recent attempts to define the concept include individual operations includes: propaganda, media manipulation, political influence, disinformation, deception, use of forgery, funding of extremist and opposition groups, spreading conspiracy theories and rumor, cyber-attacks, espionage and assassination. While the broader definition offered by Andrew and Mitrokhin is better suited for active measures’ adaptable nature, these operations all fall under the larger umbrella of active measures and offer clarity on what can be described as an active measure operation.

Martin Libicki, a prominent cybersecurity expert working for RAND Corporation, noted the difficulty with another equally important concept, information warfare. In 2007, he wrote “that well over a decade after the topic of information warfare broke out into the open, its conceptual underpinnings remain weak and largely unsatisfactory, with fierce battles raging over neologisms and definitions.” Considering the definitional variations

for information warfare, this thesis contextualizes it as a component of hybrid warfare and conducted through the use of active measures. M.M. Taraskin and S.A. Cheshuin, who both contributed to Russia’s National Security Concept of the Russian Federation adopted in 1999, wrote an article in 2009 for the journal, *Vestnik Akademii Voyennykh Nauk* (Bulletin of the Academy of Military Sciences) which described information warfare.\(^{36}\) The authors define information warfare as a “struggle in the information sphere to impact the opposing side’s information objects and protect one’s own information objects from such impact.”\(^{37}\) They continue to make an important distinction, noting that information warfare includes, “all the means and methods of impacting information, information-psychological, and information-technological objects and information resources to achieve the objectives of the attacking side.”\(^{38}\) The distinction between information-psychological and information-technical can be explained as the use of the media to impact the consciousness of individuals and groups as opposed to the use of software and communication technologies to disrupt mass media as well as military and civilian information networks.\(^{39}\)

Malign influence operations or simply influence operations, are another type of active measure that is crucial to understanding attempts to disrupt or influence elections but suffers from definitional ambiguity. An in-depth examination conducted by a team of researchers from the RAND Corporation in 2009 provides the most inclusive definition which again is beneficial given active measures adaptive nature. They described


\(^{37}\) Ibid.

\(^{38}\) Ibid.

\(^{39}\) Ibid.
influence operations as “the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviours, (sic) or decisions by foreign target audiences that further [a nation’s] interests and objectives.””

Given this wide spectrum within influence operations, it is also clarifying to establish the different types of propaganda used to advance the operation. In *Propaganda and Persuasion*, Garth Jowett and Victoria O’Donnell outline propagandas severity based on color. They describe white propaganda as coming from a “source that is identified correctly, and the information in the message tends to be accurate…Although what listeners hear is reasonably close to the truth, it is presented in a manner that attempts to convince the audience that the sender is the ‘good guy’ with the best ideas and political ideology.”

While black propaganda also known as disinformation is described as “credited to a false source, and it spreads lies, fabrications, and deceptions.” Falling in between those extremes exists gray propaganda, in which “the source may or may not be correctly identified, and the accuracy of information is uncertain.”

Given the long history of intelligence operations, difficulties with definitions can arise for a variety of reasons, including translation issues and imprecision by those in the media. With these definitions describing various aspects of intelligence operations firmly established, it is possible to pivot to cyber aggression and security which have become an

---

42 Ibid.
43 Ibid.
integral part of modern intelligence operations. Yet, here too, definitional imprecision has led to a lack of clarity on the part of the public which is only slowly being reversed as cybersecurity becomes a more common concern for society.

**Cyber Aggression & Security**

The most basic definitions set the perimeters of the discussion on cyber issues. “Cyberspace” as was recognized in the 2014 Department of Defense Dictionary of Military and Associated Terms is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” While a “cyber-attack” is understood by the National Institute of Standards and Technology as “an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.” This definition of cyber-attack proves most relevant as it accounts for the increasing nuance of cyber-attacks and does not exclude the possibility of maliciously controlling or destroying controlled information as a form of attack.

Yet, even with this inclusive definition of cyber-attacks, it is noteworthy that many international security organizations, NATO included, are moving towards the more common use of cyber operations. As NATO’s Tallinn Manual on the International Law

---


Applicable to Cyber Warfare published in 2013 indicates, cyber operations are “the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.” This increasing preference for describing actions as cyber operations rather than cyber-attacks is an indication of cyber operation’s increasing complexity. Part of that complexity, is related to the rise of “internet trolls” or just “trolls” who are responsible for cyber operations. An internet troll in its most benevolent form can be “a person who posts incendiary comments with the express purpose of provoking an argument.” NATO’s StratCom Centre of Excellence researchers have created a new term, the “hybrid troll,” to acknowledge the trolls which operate as “hired, pro-Russian trolls, communicate a particular ideology and, most importantly, operate under the direction and orders of a particular state or state institution.” The researchers claim while a standard troll has “no apparent instrumental purpose,” “the aim of hybrid trolls has been to promote the Kremlin’s interests and portray Russia as a positive force against the ‘rotten West’ and the US hegemony.”

These hybrid trolls are also extremely well equipped. One of the tools at their disposal is what is known as “automated internet bots” or “bots”, and in particular, one class of internet bot known as the “Socialbot.” Techopedia offers a concise definition for internet bot as “software that performs an automated task over the Internet. More

---


49 Ibid.
specifically, a bot is an automated application used to perform simple and repetitive tasks that would be time-consuming, mundane or impossible for a human to perform.”

For socialbots, Techopedia offers a more fulsome definition, which is indicative of the controversy socialbots cause within the tech industry, it describes them as:

A type of bot that controls a social media account. Like all bots, a socialbot is automated software. The exact way a socialbot replicates depends on the social network, but unlike a regular bot, a socialbot spreads by convincing other users that the socialbot is a real person. If not malicious, most would at least argue that socialbots are unethical.

After all, their whole point of social networking is for actual humans to connect. Whether or not a socialbot actually steals data or is just done for amusement of the creator, the fact of the matter is that a socialbot needs to trick a real user in order to spread. … Socialbots are most common in Twitter, though there also have been experiments with Facebook bots. Given the design of Twitter with short messages, re-tweeting, following etc., it's actually not too difficult for a socialbot to appear human. Identity theft is a huge concern with socialbots, but what really differs from other forms of malware is the trust factor that exists in social networks. This can serve to help the socialbot spread, but also

---

brings up questions as to whether a botnet of socialbots could influence external events.”

To add to their effectiveness, hybrid trolls will also employ large numbers of socialbots in what is called a “botnet.” Techopedia again offer a succinct definition, describing botnets as “a group of computers connected in a coordinated fashion for malicious purposes. … These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.

Hybrid trolls, working under the direction of a state, are often, reportedly, organized into teams and provided with work space and schedules to maximize their efficiency. While sources are incredibly difficult to come by as no nation is willing to confirm the existence of clandestine cyber operation facilities, journalists working for the Russian independent newsmagazine RBC were able to uncover details through a sting operation. Polina Rusyaeva, Andrey Zakharov, and Ludmila Savchuk gained employment at what has been described as the Internet Research Agency in St. Petersburg Russia and shared the details of the experience with Western journalists to further promote their discoveries. The journalists claim that the agency employed up to 400 hybrid trolls and enjoyed a monthly budget of at least 20 million rubles (approximately $400,000) a month. Their accounts offer intimate details and if credible confirm many of the details

---

54 Ibid.
55 Ibid.
offered by security firms and intelligence agencies about Russia’s state-sponsored cyber operations.

Recognizing the growing role of cyber operations as a critical aspect within influence operations, NATO’s Cooperative Cyber Defence COE researchers coined the term “influence cyber operations (ICO).” They define ICOs as “encompass activities undertaken in cyberspace affecting the logical layer of cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences.” Some of the verifiable methods used to accomplish these ICOs is documented by TrendMicros, SecureWorks, and Microsoft and addressed in following chapters include structured query language (SQL) injections, spear-phishing emails, distributed denial-of-service attacks, data dumps (or political doxing) and astroturfing. As not all these methods are commonly known, they will be defined to ensure clarity in future chapters. SQL injections and spear-phishing emails are methods to gain unauthorized access to a target’s database. An SQL injection occurs when an “attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application’s database server,” and represents one of the most common ways malicious actors gain access to a private database. Similarly, a spear-phishing email grants perpetrators access to the target’s private database through the use of “fraudulent emails, containing malicious code, target specific organizations in an effort to gain access to confidential

---


A denial-of-service attack often requires the use of botnets but uses brute force to “make an online service unavailable by overwhelming it with traffic from multiple sources.” The remaining methods, data dumps (or political doxing) and astroturfing make use of stolen and controversial information or disinformation to further the ICO’s objective. A data dump, which has also been described as a form of doxing, entails the release of potentially stolen information at a time when it is determined to have the greatest repercussions on the victim. While astroturfing, playing of the concept of grass root organizations, attempts to supporting a divisive group or causes through the use of botnets and hybrid trolls.

Together, these sections offer a comprehensive overview of terms related to intelligence operations and cyber aggression and security which are relevant for the following chapters. Unfortunately, both the fields of intelligence and cyber security are complex and the precise meaning of a term or phrase can be diluted when used improperly by the broader public. By providing the definitions and the reasoning behind why certain definitions were chosen, this chapter offers greater clarity and specificity on subjects which have remained opaque to the wider public.

Chapter Four: Types of Cyber Operations

While this thesis broadly identifies the role of cyber operations in disrupting and influencing elections in democratic states, the common denominator in these cyber operations has been the Russian Federation. Due to limitations in publicly available information, this thesis does not attempt to attribute specific operations against democratic states’ elections to Russia. However, given the depth of literature and data documenting Russian involvement, a great deal of clarity on the different types of cyber operations can be gained by examining verifiable Russian cyber operations meant to disrupt or influence elections in the U.S. and Europe.

Testifying before a Senate Judiciary subcommittee hearing on Russian interference in the U.S. 2016 presidential election, former Director of National Intelligence, James Clapper Jr. provided the lawmakers present with the collective assessment of the FBI, CIA and NSA. Clapper explained “that the Russian government pursued a multifaceted influence campaign in the run-up to the election, including aggressive use of cyber capabilities.”62 Later in the hearing, in response to an assertion by Senator John Kennedy of Louisiana that the Russians had been running these types of campaigns for years, Clapper rejected the assertion, indicating that “this is unprecedented in terms of its aggressiveness and the multifaceted campaign.”63 Likewise, in a statement prepared for the U.S. Senate Select Committee on Intelligence in 2017, Director of NATO Strategic Communications Centre of Excellence, Janis Sarts explained how new

---

63 Ibid.
technological developments made these cyber operations attractive because they were increasingly fast, cheap, and geographically unlimited. Director Sarts, further supported this point by putting forward a chronology of cyber operations which targeted European elections as documented by NATO StratCom COE including efforts in: Estonia in 2009, Ukraine in 2014, Germany in 2015, Montenegro in 2016, and the Netherlands, Norway and France in 2017.

A crucial element in understanding cyber operations and why they prove effective is related to the actual perpetrator of the operation. These perpetrators of cyber operations, or trolls as they’re know in cyber security parlance, can operate from any nondescript location with an internet connection, are relatively inexpensive to employ and do not require extensive investment to maximize their cyber capabilities. Despite claims from the Kremlin denying any state involvement in cyber operations targeting other country’s domestic elections, there is mounting evidence that indicates the existence of Russian state-sponsored facilities designed to conduct cyber operations on a massive level. The activities of Russian-sponsored cyber operation facilities, or troll farms again as they’re referred to in cyber security parlance, has been documented and tracked by several European intelligence agencies, including the United Kingdom’s House of Commons Defence Committee, Czech Republic’s Security Information Service

---


65 Ibid.


(BIS), Estonia’s Kaitsepolitseiamet (Estonian Intelligence Services) and Sweden’s Sakerhetspolisen (Swedish Security Services) for the past several year.  

One of the most authoritative and thorough source of information on the existence of these Kremlin-sponsored facilities comes from the U.S. Special Council investigation of Russian interference in the 2016 U.S. elections led by Robert Mueller III. In a recent indictment, Mueller’s team charged the Russian organization, the Internet Research Agency LLC, and thirteen Russians affiliated with the organization for having “knowingly and intentionally conspired … to defraud the United States by impairing, obstructing and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016.” The indictment goes into granular detail, outlining the agency’s organizational structure, protocols, budget and its work in the creation of false American personas, social media accounts, groups and events. And while it’s important to remember that an indictment is only a formal accusation brought


73 Ibid.
about by a federal prosecutor, the incredible specificity of the charges in the indictment indicate the underlying sources were provided by cooperative U.S. intelligence agencies. 

As new details and sources on the methods used to interfere in the U.S. 2016 presidential election emerge, former Director of National Intelligence, James Clapper’s choice of the phrase “multifaceted campaign” appears exceedingly appropriate. To organize the different types of cyber operations utilized to interfere in elections, it is clarifying to establish the types of cyber operations based on their intended targets. With currently available public information, it’s possible to create three categories of operations: cyber operations which targeted voting equipment and election infrastructure, cyber operations which targeted elected officials, political operatives and political parties and cyber operations which targeted the public. The following details the specific operations which fall in each category.

Targeting Voting Equipment and Election Infrastructure

As it has been seen elsewhere, the available public data on intrusions into voting equipment and its online infrastructure is limited but becoming increasingly available through the declassification of information. It is reasonable that few nations want to provide details of the vulnerabilities that exist within their electoral infrastructure and voter registration databanks. However, it is noteworthy that this method of compromising the physical election hardware does not seem to be the preferred method as it is detectible and not as effective as other methods yet to be discussed.

In the U.S. there have been several sources which implicate Russian actors in the probing of US election-related infrastructure and voter registration systems across various
states. The Acting Deputy Undersecretary for Cybersecurity and Communications at the DHS, Jeanette Manfra claimed the nation’s cyber systems are under constant attack, indicating the DHS had evidence of cyber-enabled scanning and probing of election related infrastructure originating from servers operated by Russian company.\textsuperscript{74} In testimony to the Senate Select Committee on Intelligence, Manfra continued to describe unclassified FBI material which gave specific details regarding a cyber-attack in July 2016 that resulted in a State Board of Elections website being compromised.\textsuperscript{75}

That FBI material, originally classified because it contained actionable IP addresses, was a flash warning issued by the FBI Cyber Division to all the states’ Board of Elections. In the bulletin, the FBI warns of two cyber-attacks in July and August 2016 against unnamed (but since identified as Arizona\textsuperscript{76} and Illinois\textsuperscript{77}) states’ Board of Election websites.\textsuperscript{78} The bulletin offers the following technical details:

In late June 2016, an unknown actor scanned a state's Board of Election website for vulnerabilities using Acunetix, and after identifying a Structured Query Language (SQL) injection (SQLi) vulnerability, used SQLmap to target the state website. The majority of the data exfiltration


\textsuperscript{75} Ibid.


occurred in mid-July. There were seven suspicious IPs and penetration testing tools Acunetix, SQLMap, and DirBuster used by the actor.\textsuperscript{79}

The Structured Query Language (SLQ), as a reminder, is “computer language designed for eliciting information from databases.”\textsuperscript{80} While the SLQ Injection (SLQI) is the process of finding vulnerabilities in the SLQ and inserting malicious code giving the user the ability to tamper with the existing data across the database, in this case, the databases maintained by both Arizona and Illinois’s Board of Election.\textsuperscript{81} It’s also helpful to understand that the tools, Acunetix, SQLMap, and DirBuster are commonly used opensource web tools. They can be used to access and manage a database’s SQL, exploit the vulnerabilities within that database and insert malicious SQLIs, and map that database’s structure, directories and files, respectively.\textsuperscript{82,83,84} Equally important, all seven of the listed IP address in the bulletin have been independently identified and flagged as associated with Russian government cyber actors and Russian malicious cyber activity by the DHS’s U.S. Computer Emergency Readiness Team (US-CERT).\textsuperscript{85} The most crucial piece of information being the data exfiltration, which in an open letter to the state

\textsuperscript{83} “SQLmap: Automatic SQL Injection and Database Takeover Tool.” \textit{SQLmap.org}. http://sqlmap.org/.
Election Authorities the Director of Voting and Registration Systems for Illinois State Board of Elections, Kyle Thomas, identified as an unknown amount of voter records.  

In various European elections as well, there is evidence of successful attempts to compromise election infrastructure. One of the first well documented cyber-attacks in Europe occurred in 2014 prior to the Ukrainian national elections and also serves as a perfect example of what military experts have called hybrid warfare. The context of the attack is critical. On November 21st, 2013, Ukrainian Pro-Russian President Viktor Yanukovych suspended preparations for the implementation of an association agreement with the European Union which sparked escalating protests across the country. By February, 24th, 2014, 84 Ukrainians had died in the protests, a new interim president was named in Kiev, new presidential elections were scheduled for May and most importantly Yanukovych had fled to escape a warrant for his arrest over his involvement in the death of the protesters. Almost simultaneously as Yanukovych went into hiding, unrest and conflict fueled by allegedly pro-Russian separatists began to spread in Crimea and the eastern regions of Donets and Luhansk. These alleged pro-Russian Ukrainian separatists forces which were later identified as partially composed of and heavily

---


In this tumultuous atmosphere, an online group known as “CyberBerkut,” named after the riot police unit which had been accused of brutality against protesters at the onset of the unrest, began probing the Ukrainian Central Election Commission (CEC).\footnote{Coker, Margaret, and Paul Sonne. “Ukraine: Cyberwar's Hottest Front.” \textit{Wall Street Journal}, Dow Jones & Company, 9 November 2015. www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.} The attacks intended target was the election analytics system that aggregates voter data\footnote{“СБУ ліквідувала вірус, що мав знищити результати виборів (The SBU Eliminated a Virus that was Supposed to Destroy Election Results).” \textit{Українська правда (Ukrainian Pravda)}, 23 May 2014. www.pravda.com.ua/news/2014/05/23/7026217/}. While the technical details of the attack are scant, Volodymyr Zverev, Head of the State Service for Special Communication and Information Security, told Ukrainian reports that a virus had destroyed all of the internal data of the CEC on May 22.\footnote{Ibid.} In the aftermath of the attack it was discovered that in the attack, just three days prior to the election, CyberBerkut had infiltrated the CEC’s election infrastructure, disabled the election analytics system and released the details of the analytic system and personal contact information from the election committee staff.\footnote{Ibid.} While the CEC’s data had been backed up earlier in the day, preventing the intended delay in election results, the attack stands as one of the most brazen attempts to disrupt elections through the election infrastructure.\footnote{Clayton, Mark. “Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers.” \textit{Christian Science Monitor}, 17 June 2014. www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.}
Similar attempts have been uncovered in other European capitals as well, in particular Amsterdam. In the run up to the Netherlands’ 2017 general election, Foreign Affairs Minister Bert Koenders warned that the Dutch General Intelligence and Security Services (AIVD) were on the highest alert for cyber intrusion in the election. In fact, the AIVD warned that “the Netherlands’ Highly developed ICT infrastructure makes our nation an attractive channel for cyber-attacks.” Ultimately, after Minister of Home Affairs Ronald Plasterk, issued a warning that there had been international indications that the Russians were probing the elections, the government decided the prudent decision was to forgo the electronic system and use traditional paper and pen methods.

As it has been seen in these accounts, there are several weaknesses in targeting the physical election infrastructure and voter registration databases. Primarily, country’s intelligence agencies are constantly searching for these types of intrusions and they leave a clear trail back to the perpetrator. As it will be seen in the following section, unlike cyber operations that simply attempt to alter or interfere with the physical election infrastructure, other types of cyber operations have proven more effective in influencing elections’ outcomes and are better suited to take advantage of democratic societies’ internal divisions.

---

Targeting Elected Officials, Political Operatives and Political Parties

Cyber operations which target elected officials or candidates, their staffs, political operatives and political parties, due to the outcry of the victims of such operations, are often the most publicized. While there have been a number of extremely high-profile examples, notably in the U.S. and France, which fall within this type of operation, they have also been used to great effect in Eastern Europe while avoiding excessive international scrutiny. These operations are also often potent because there is frequently a domestic constituency which finds the operation advantageous to its own objectives.

The most infamous instance of a cyber operation used against a political target with the objective of disrupting or influencing an election occurred during the U.S. 2016 presidential election. The intense debate and scrutiny over this occurrence has also led to a significant amounts of intelligence information being released to the public which has served to inform this thesis. On January 6th, 2017, the Office of the Director of National Intelligence issued a comprehensive joint report in collaboration with the CIA, NSA and FBI entitled “Assessing Russian Activities and Intentions in Recent U.S. Elections” to the Senate Select Committee on Intelligence. As indicated in the title, this report offered the agencies’ collective assessment on Russia’s involvement in the 2016 U.S. elections but also revealed the granular details of the Russian cyber operations.

The assessment indicated that in the early stages of the operation, “Russia’s intelligence services conducted cyber operations against targets associated with the 2016 U.S. presidential election, including targets associated with both major US political
This point suggests that in the earliest stages the operation was intended to cause disruption to the election process, rather than assist any one candidate. The report continues to name the Russian intelligence agency, the General Staff Main Intelligence Directorate (GRU) as one of the main actors in the cyber operation and outlines its broad efforts to collect information from “US primary campaigns, think tanks and lobbying groups they viewed as likely to shape future US policies.” The assessment claims that the GRU had gained access to the Democratic National Committee (DNC) networks from July, 2015 to June, 2016 through the use of personal email accounts of Democratic Party officials and political figures and that by May they had used this access to exfiltrate large volumes of data. The cyber security company, Secureworks, was able to track the attack back to Russia intelligence affiliated IP addresses with moderate confidence. Securework’s Counter Threat Unit analyzed 3,907 individual Gmail accounts and corporate and organizational email accounts that use Gmail as a service associated with the 2016 U.S. presidential campaign and determined that the perpetrators used what is known as a spear-phishing attack to gain entry to the DNC’s networks. The attack involves sending deceptive emails to higher level staff members, prompting the victim to enter security information to resolve a fictitious issue, upon providing the security information the perpetrator gains access to the network. The Counter Threat Unit also uncovered similar efforts associated with Germany’s Prime Minister Angela Merkel and

102 Ibid.
103 Ibid.
105 Ibid.
rival candidates Donald Trump, Bernie Sanders, Ted Cruz, Marco Rubio and John Kasich which again strongly indicates that the purpose of these operations was to disrupt the election process.106

A similar operation took place during the 2017 French presidential election. Context is quite important here. On the far-right, The Front National’s (FN) candidate Marine Le Pen held a consolatory position on Russia.107 A Eurosceptic and ultra-nationalist, Le Pen had defended Russian action in Ukraine and Syria and called for a “balanced” relationship between Russia and Western powers.108 While Emmanuel Macron, considered a political centrist, held pro-EU views and had been supportive of the EU sanctions placed on Russia over its aggression in eastern Ukraine.109 According to an assessment report conducted in the aftermath of the operation by TrendMicro, a cyber defense company, candidate Macron and his political party, La République En March!, were targeted in cyber operations.110 The report describes similar methods as used in the cyber operation that targeted the DNC, including the use of spear-phishing attacks against higher level staff members to gain access to private information within the campaign’s database.111 While the perpetrators were operating under a different moniker,

---

108 Ibid.
111 Ibid.
PawnStorm, TrendMicro has claimed with fair confidence that the attack can be traced back to Russian GRU affiliated IP addresses.112

The assessment which was released in the aftermath of the 2016 U.S. election, indicated that “The Kremlin’s campaign aimed at the US election featured disclosures of data obtained through Russian cyber operations; intrusions into US state and local electoral boards; and overt propaganda. Russian intelligence collection both informed and enabled the influence campaign.”113 That final sentence is critical to understand how the stolen data was then weaponized and used against the political organization from which it was stolen. It also serves as a segue into the next type of cyber operation.

Targeting the Public

Evidence of cyber operations conducted against the broader public in an effort to interfere in elections is becoming increasingly available. These types of cyber operations are designed to influence the voting population and promote the most extreme views within a society. In 2016, Pascal Brangetto and Matthijs Veenendaal of the NATO Cooperative Cyber Defence Centre of Excellence, proposed the term “Influence Cyber Operations” (ICOs) for this new type of operation which adapted elements of influence operations, a tool used by international intelligence services for decades, and integrated them with emerged cyber operations.114 The advent of “cyberspace offers numerous

possibilities for these kinds of coercive operations, which are designed to influence a target audience by changing, compromising, destroying, or stealing information by accessing information systems and networks.”

Keir Giles, a senior fellow of the Russia and Eurasia Programme at Chatham House, specifies three ways ICOs prove effective: by “both internally and externally focus[ing] media with a substantial online presence,” by “target audiences on a broad front in their own language” and also by “use of social media and online fora as a force multiplier to ensure Russian narratives achieve broad reach and penetration.”

One tool which acts as a force multiplier and amplifies the effect of ICOs is the social bot. While social bots operate in a definitional fog, this thesis uses a definition which focuses on certain qualifying aspects of the computer algorithm. These aspects include: the program can be fully automated as well as partly controlled by human action, autonomous agent-like action, an orientation toward a goal, can operate on multiple modes of communication, and operates in a wider social media ecosystem. In a written response to questioning by the U.S. Senate Select Committee on Intelligence, Facebook’s Vice President and General Counsel Colin Stretch claimed that “in October 2016, for

---


example, we disabled about 5.8 million fake accounts in the United States” adding, “At the time, our automated tooling did not yet reflect our knowledge of fake accounts focused on social or political issues.” An admission, which as Senator Mark Warner pointed out, could mean the numbers initially reported only account for a fraction of the actual number of fake accounts. Stretch further claimed that learning from the US election led to the detection of bots being used in European elections. He indicated that in advance of the 2017 French presidential elections more than 30,000 accounts had been exposed while prior to the 2017 German federal elections “tens of thousands” of accounts had been uncovered. The report also noted while Facebook has been working fastidiously to remove fraudulent accounts, it continued to uncover them on a daily basis.

Stretch also advised the lawmakers to examine the techniques used to amplify divisive messages as outlined in the white papers on information operations released in April, 2017. In its findings Facebook admitted that social bots were a tool utilized by individuals, and as Facebook claims, Russian-linked accounts, to further advance information operations on the platform. Facebook asserts that these accounts used social bots to amplify their reach by: the masse creation of fake accounts, coordinated sharing and reposting of content across multiple pages, coordinated and repeated

---

120 Ibid.
121 Ibid.
122 Ibid.
123 Ibid.
commenting sometimes in a harassing manner, coordinated “likes” or reactions, coordinated astroturfing of groups, creation of groups and pages with the specific intent to spread sensational and bias headlines which often distorted facts and creations and distribution of inflammatory and occasionally racist memes, manipulated photos and video content. One of the most important findings, was the realization that while these social bots can act entirely autonomously, they were more frequently used to promote and amplify the content of a specific account which indicates that individual hybrid trolls often operate with a network of social bots supporting the troll’s objective.

Yet, this activity is not contained solely to Facebook. Additional popular social media outlets like Instagram, Reddit, Google, Twitter and YouTube have all reported evidence of Russian troll farms’ activities on their platforms. In his statement to the U.S. Senate Select Committee on Intelligence, Stretch also gave a broader assessment of the situation, explaining that “foreign actors, hiding behind fake accounts, abused our platform and other internet services to try to sow division and discord—and to try to undermine our election process— [which] is an assault on democracy.” In his testimony, Stretch indicated that Russian hybrid trolls misrepresenting themselves as U.S. citizens created and shared posts, paid to advertise and promote their specific pages, and paid for specific advertisements to be seen in other users News Feeds. While at a

---

128 Ibid.
different session of the same committee, the Acting General Counsel for Twitter, Sean Edgett, recounted similar activities also occurring on Twitter’s platform. During the testimony, Edgett also elaborated on the use of Russian spam, fake accounts and automated bots on Twitter, all of which were used to amplify the reach of their disinformation.

A presentation from the Chairman of the Committee, Senator Richard Burr, also demonstrated how these efforts to sow division among U.S. citizens could and on occasion had moved from social media platforms to public space. His presentation outlined how two Russian-sponsored groups, “Heart of Texas” and “United Muslims of America” managed to organize rival rallies at the same location and time in Houston, Texas which led to confrontation and disruption in the streets of an American city. A presentation by the Vice Chairman of the Committee, Senator Mark Warner, displayed Russian-produced content by a group named “Army of Jesus” which featured Hillary Clinton depicted as Satan in a boxing match with Jesus. Besides disparaging one of the candidates, Senator Warner’s presentation also demonstrated how Russian-sponsored

---


130 Ibid.

131 Ibid.

pages on social media platforms served to spread Russian disinformation more broadly by linking users to pseudo-news websites also maintained by Russian accounts.\textsuperscript{133}

Despite all the methods used to amplify divisive messages produced by hybrid trolls, their most effective method of advancing an ICO may also be their most straightforward, the data dump or, as it is sometime referred to, political doxing. As described in the prior section, hybrid trolls have a variety of methods to gain unauthorized access to candidates, political operators and political entities’ databases. While these political actors are increasingly aware of the vulnerabilities and working to protect their databases, it only takes a small weakness in a database’s SQL or one inattentive staff member being deceived by a spear-phishing email for a determined hybrid troll to gain entry. In fact, these two methods which are both exceedingly common, were responsible for two of the most infamous data dumps to date. French candidate Emmanuel Macron and his political party, La République En March!’s database was breached through the use of a SQL injection, while in the U.S., the Clinton campaign and the DNC’s were penetrated through the use of spear-phishing emails.

These data dumps are typically timed to ensure that the potentially damaging information is released when it will have the greatest impact on the intended target. In the case of Emmanuel Macron’s campaign this meant days before the election runoff with Marine Le Pen and hours before an official election blackout which prevents the media

from reporting on the campaigns. As seen in the 2016 DNC leak, the perpetrators also
go to great lengths to hid their identity which serves to obfuscate the true intention behind
making the data public. The GRU affiliated persona “Guccifer 2.0,” provided the data
with a third-party website, DCLeaks.com, which then moved the data along to Wikileaks
and the broader public. Finally, once the data reaches the public sphere, the hybrid
trolls with the assistance of botnets work in a coordinated manner to ensure it is amplified
and reaches as broadly as possible.

As seen in this chapter, cyber operations are extremely adaptable and can be
useful to intelligence services in a number of different ways. By utilizing cyber
operations, a malicious actor or state can target election infrastructure, political
operatives, elected officials, political candidates, political organizations as well as the
broader public. While cyber operations can stand alone as a potent tool of intelligence
agencies, they also have been used to support other types of active measures such as
political influence operations and disinformation operations. Most alarmingly, there is no
indication that cyber operations’ versatility has reached its limit. In fact, it’s likely that as
social, political and business interactions increasingly transpire within cyberspace, cyber
operations will continue to find new vulnerabilities to exploit.

---

Chapter Five: Purpose behind the Cyber Operations

As evidence of the Russian Federation’s use of cyber operations to disrupt or influence elections has become increasingly verifiable, the key question still to be answered is “why?” Why has Russia engaged in these cyber operations against elections? What was the purpose behind these cyber acts? Fortunately, an examination of Soviet history and current Russian national security doctrine offers an incredible amount of insight which can help answer these questions.

Cyber operations designed to interfere in elections have been, by necessity, largely conducted as covert operations. It is important to remember that the reliance of aggressor states, in particular Russia, on covert operations like disinformation operations and cyber operations are not demonstrations of military strength. They are rather an adaptation meant to counter the superior conventional military strength of rival nations. This assertion is well supported by national military expenditure data, as in 2016 Russia spent under $83 billion on defense compared to the U.S. which spent over $611 billion.  

By comparison, the Russian defense expenditure makes it a closer rival to Saudi Arabia which spent over $63 billion. Russia’s defense budget is also outmatched by the combined expenditure of the United Kingdom and France which together spent just under $113 billion on defense in 2016.  

Unable to oppose the U.S. and its European allies in a conventional military confrontation, rival nations use nonconventional methods that are available. Nonconventional or asymmetrical methods of warfare, both new and old, have historically been the domain of state intelligence agencies. When considering the attack

---

138 Ibid.
on democratic states’ elections, it is more helpful to view cyber acts as the newest type of operation at the disposal of intelligence agencies rather than a new type of warfare.

Russia and its predecessor, the Soviet Union, have throughout its history understood the crucial role nonconventional warfare could serve while facing a militarily superior opponent. In 1920, Vladimir Lenin wrote:

The most powerful enemy can be vanquished only by exerting the utmost effort, and by the most thorough, careful, attentive, skillful, and obligatory use of any, even the smallest, rift between the enemies, any conflict of interests among the bourgeoisie of the various countries and among the various groups or types of bourgeoisie within the various countries and also by taking advantage of any, even the smallest opportunity of winning a mass ally, even though this ally is temporary, vacillating, unstable, unreliable and conditional.\textsuperscript{139}

This mentality, of employing subversion, deception and manipulation to further the group’s goals, made tactical sense for the Bolsheviks as a small group of revolutionaries trying to overthrow the militarily superior Tsarist regime in Moscow. It evolved into the Soviet concept of \textit{aktivnyye meropriyatiya} or “active measures” and was “well integrated into Soviet policy and state structure, not only the KGB.”\textsuperscript{140} The U.S. Information


Agency elaborated on the different types of Soviet propaganda in a report to Congress in 1988. The agency outlined three gradations of propaganda:\textsuperscript{141}

1.) Black propaganda which was disseminated by the KGB and composed of disinformation and forgeries meant to support a disinformation operation’s authenticity.\textsuperscript{142}

2.) White propaganda which was disseminated by elements of the Soviet press under the Propaganda Department of the Central Committee which generally maintained accuracy but supported the themes developed by active measures operations and framed their reports from a heavily pro-Soviet perspective.\textsuperscript{143}

3.) Gray propaganda which was disseminated by the International Department (ID) of the Soviet Communist Party Central Committee, local communist groups, Soviet-backed international front groups, workers organizations and foreign-policy related academic institutions and contained both elements of truth and disinformation.\textsuperscript{144}

Further evidence supporting the centrality and importance of active measures operations in the Soviet security apparatus come from the long-standing head of the active measures operations for the East German Stasi, Colonel Rolf Wagenbreth. The Colonel practically echoed Lenin’s words, when he reportedly said “A powerful adversary can only be

\textsuperscript{142} Ibid.
\textsuperscript{143} Ibid.
\textsuperscript{144} Ibid.
defeated through ... sophisticated, methodical, careful, and shrewd effort to exploit even the smallest ‘cracks’ between our enemies ... and within their elites.”\textsuperscript{145}

During the Cold War, the U.S. intelligence community worked fastidiously to identify and counter Soviet active measures operations. In an FBI report to the House of Representatives in 1981, only declassified by the CIA in 2006, the agency outlines the different types of known active measures operations at the time, which include: efforts to manipulate the press in foreign countries, disinformation operations, political influence operations, forgery operations, and efforts to influence local groups such as arms control and disarmament movements, labor organizations, trade unions, religious organizations.\textsuperscript{146}1\textsuperscript{47}

According to an FBI report declassified in 2013, Soviet forgery operations were conducted with several goals in mind. They served to promote Soviet foreign policy goals, influence political action and public opinion in the U.S. and abroad and discredit the U.S. and its allies.\textsuperscript{148} These forgery operations typically targeted elected officials and the heads of government agencies from NATO-member countries. The falsified documents would then be widely circulated through cooperative pro-Soviet media outlets as well as unwitting international media outlets. Most frequently, the forgeries were

\textsuperscript{148} Ibid.
designed to supply ‘factual evidence’ for Moscow’s disinformation campaigns which had already been advanced by other active measure operations and propaganda. One example of alleged Soviet forgery came in the form of a letter sent anonymously to the Washington Post and U.S. New and World Report in 1986. The purported forgery was authored by the United States Information Agency (USIA) official Herbert Romerstein to Senator David Durenberger, the former Chairman of the Senate Select Committee on Intelligence. The letter callously suggests that the USIA would inflate the reported number of Chernobyl victims in an effort to further discredit the USSR over the incident. The letter, having its intended effect, created an immediate public outcry from the European NATO-members even though it was immediately and thoroughly denied by all involved parties.

In 1987, the FBI described political influence operations as one of the most increasingly common and sophisticated active measure programs utilized by the Soviet Union’s security apparatus. Soviet agents would secure the assistance, often unwittingly, of European and U.S. citizens who held similar foreign policy goals on specific issues as the Soviet Union. By misrepresenting themselves as religious leaders, trade representatives, journalists, UN officials or diplomats, the Soviet agents would both help establish and provide material aid for groups which held foreign policy

150 Ibid.
151 Ibid.
152 Ibid.
153 Ibid.
154 Ibid.
positions favored by Moscow. These operations also varied in size. In some instances, Soviet operatives would target political figures in a foreign country by playing to their ego, offering meetings with high-level Soviet leaders, then exploiting the connection by disseminating a mixture of distorted truths and falsified information which was designed to advance Soviet foreign policy goals or by blackmailing the target to extract information. While in other instances, a political influence operation was directed at the broader public through influencing prominent journalists. In one such case, a prominent French journalist, Pierre-Charles Pathe, a prolific writer and an influential voice in French political circles, was under Soviet patronage for over twenty years before the influence operation was detected by French intelligence agencies and Pathe was arrested.

As established in previous chapters, technological adaptation, specifically the integration of cyber operations within intelligence agencies, has led to an unprecedented amplification of political influence operations by taking full advantage of the reach provided by online social media. In bypassing the journalist who once stood as the gatekeepers to the wider public, these operations were able to craft their messaging more precisely, reach a significantly larger portion of the population and disseminate disinformation with significantly greater frequency. Today’s influence operations employ

---

156 Ibid.
158 Ibid.
159 Ibid.
a number of different methods which have amplified their messages. Popular social media outlets like Facebook, Instagram, Reddit, Google, Twitter and YouTube have all reported evidence of Russian troll farm activities on their platforms. In a statement to the U.S. Senate Select Committee on Intelligence, Facebook’s Vice President and General Counsel Colin Stretch claimed “foreign actors, hiding behind fake accounts, abused our platform and other internet services to try to sow division and discord—and to try to undermine our election process—is an assault on democracy.” In his testimony, Stretch indicated that Russian trolls misrepresenting themselves as U.S. citizens created and shared posts, paid to advertise and promote their specific pages, and paid for specific advertisements to be seen in other user’s News Feeds. While at another secession of the same committee, the Acting General Counsel for Twitter, Sean Edgett, indicated that similar activates were also occurring on Twitter’s platform. During the testimony, Edgett also elaborated on the use of Russian disinformation, fake accounts and social bots on Twitter, all of which were used to amplify their divisive messages.

Russia’s continued strategic use of active measures against rivals and its increasing use of cyber operations is not only supported by evidence provided by the

162 Ibid.
164 Ibid.
intelligence services countering Russia’s aggression. In fact, these disruptive and covert methods were written into the Russian National Security Strategy, a presidential edict issued by Vladimir Putin in December, 2015. In the security strategy document, Russia’s vision of its resurgent position and disruptive role in the international system becomes apparent even while invoking language which promotes global cooperation and sustainable development. When addressing Russia’s role in the modern world, the security strategy emphasizes enhancing its role in shaping a polycentric world, protecting the rights of compatriots abroad and maintaining and strengthening its economic potential in the face of restrictive economic measures introduced by other countries. While written with conciliatory language, some of these aims are quite clear. Enhancing Russia’s role in a polycentric, or multipolared world, requires the degradation of the US and its allies which according to the security strategy “are seeking to retain their dominance in world affairs.” Protecting the rights of compatriots abroad may sound benevolent, yet recent history in Georgia, Crimea and eastern Ukraine demonstrate that the desire to protect ethnic Russians can be used as a justification for military intervention within neighboring countries. Strengthening Russia’s economy in the face of economic restrictions, while unconfrontational in tone, also indicates Russia’s continued defiance against the economic sanctions imposed over its annexation of Crimea in 2014. These three clauses, read together, point to ongoing confrontation on the global stage as Russia continues to defy international law in the face of sanctions, remains a military threat to its neighbors and attempts to undermine the existing international order.

---


166 Ibid.
The security strategy document specifies a number of Russian national defense priorities, however these defensive concerns mirror Russia’s own tactics in their efforts abroad. While allegedly addressing a security concern, one particular section regarding informational and communication technologies reads more like a succinct description of Russia’s own strategy. It states, “The intensifying confrontation in the global information arena caused by some countries’ aspiration to utilize informational and communication technologies to achieve their geopolitical objectives, including by manipulating public awareness and falsifying history, is exerting an increasing influence on the nature of the international situation.” Similarly, the document points out potential security risks associated with the use of financial and business ties as well as energy policy as a means of political manipulation, all of which, are tactics Russia has been accused of using itself. While the document does temper its language at certain points, it openly calls into question the viability of the Euro-Atlantic regional security system based on the collective defense of NATO and the European Union. When read in context with Russia’s recent maneuvers on the global stage, it becomes clear that this is the security doctrine of a nation with revisionist global ambitions.

As it’s national security strategy provides a broader overview of Russia’s geopolitical objectives, the Doctrine of Informational Security of the Russian Federation signed by Vladimir Putin on December 5th, 2016, offers more specific detail as to the

---

purpose of Russian cyber operations. In a manner similar to the security strategy, it outlines informational security threats that are brazenly similar to the cyber operations Moscow itself has been accused of utilizing. One section warns that “extremist organizations widely use information tools to influence individual, group and public consciousness in order to fester interethnic and social tensions, incite ethnic or religious hatred or hostility, [and] spread extremist ideology” which sounds extremely similar to the cyber operations allegedly undertaken by the GRU’s hybrid troll and social bots.170 In a section related to information security and public security, Russian authorities warn of the “use of information technologies to promote extremist ideology, spread xenophobia and ideas of national exceptionalism for the purposes of undermining the [state’s] sovereignty, [as well as] political and social stability.”171 Here lies a crucial insight, Moscow believes the use of informational technologies, i.e. cyber operations, can promote extremist ideology which in turn undermines political and social stability and ultimately a state’s sovereignty.

When one considers Russia’s historical reliance on active measures to counter rival conventional military strength, its open disdain for Euro-Atlantic regional security as provided by NATO and the European Union is clear. Russia’s promotion of corrosive extremist ideologies, political influence and disinformation via cyber operations paints a broader picture. The purpose behind these cyber operations is to amplify Russian efforts to undermine the social and political cohesion between the members of the European Union and NATO as well as between different groups within the member countries. Once

---


171 Ibid.
again, we recall Lenin, who in 1920 wrote, “the whole point lies in knowing how to apply these tactics”¹⁷² An equally important point, however is that Russian cyber operations should not be considered in isolation. They have become one of Russia’s most potent active measures, yet these active measures all work in tandem to advance Russia’s geopolitical objectives as a revisionist power.

To further support this claim, it is worthwhile to examine the political parties which have been most critical of the European Union and NATO while also holding a more conciliatory position towards Russia. In a report, the Economist tallied the European political parties in which members were known to have personal and business ties with Russia’s political elite and oligarchs and also were supportive of relations with Russia. The parties included: Attack of Bulgaria, Golden Dawn and Syriza of Greece, Jobbik of Hungary, the Freedom Party of Austria, the National Front of France, the British National Party and the UK Independence Party of the United Kingdom, Podemos of Spain, the Northern League and Forza Italia of Italy, National Democratic Party and Alternative for Deutschland of Germany and Vlaams Belang of Belgium.¹⁷³ While the U.S. Republican Party was not included in this list, President Trump has been unprecedently critical of NATO¹⁷⁴, cheered the U.K.’s referendum to leave the European

Union\textsuperscript{175} and has been uniquely open to enhanced cooperation with Russia\textsuperscript{176} all while under the shadow of special prosecutor Robert Mueller’s investigation into potential ties to Russia. Admittedly, it is impossible to determine whether politicians from these parties have been the target of political influence operations or if they genuinely held conciliatory views towards Russian foreign policy. However, such personal and business ties are strikingly similar to the connections used by Soviet agents when they ran political influence operations in the past. If any of these politicians are the targets of Russian influence operations it also supports the argument that Russia is using all the active measures in their intelligence services’ repertoire to advance their geopolitical objectives.

The claims made here are expansive. Through evaluating the body of research for this thesis, it has become clear that Russian intelligence services, experts in the use of covert active measures to advance the Russian state’s geopolitical objectives, have effectively adopted cyber operations. Russian intelligence services have used cyber operations to both enhance the viability of their political influence and disinformation activities. By using cyber operations in tandem with other active measures, Russia was able to interfere in the democratic elections of states with a particular focus on those within the transatlantic community. This disruption was meant to impact the social and political stability of these Western societies, promote those who held sympathetic views of Russia and undermine the regional security as provided by NATO and the European Union. Crucially, this assessment is shared by many who are considered knowledgeable


on the matter. On March 8th, 2018, the commander of U.S. European Command and NATO’s supreme allied commander, Cutis M. Scaparrotti addressed the Senate Armed Services Committee. In his testimony, Commander Scaparrotti claimed:

Russia seeks to change the international order, fracture NATO, and undermine U.S. leadership in order to protect its regime, re-assert dominance over its neighbors, and achieve greater influence around the globe. To achieve these ends, the Kremlin is prepared to employ the full spectrum of Russia’s power, … Additionally, Russia aggressively uses social media and other means of mass communication to push disinformation, test the resolve of the United States, and erode our credibility with European partners. … Russia is advancing its indirect and asymmetric capabilities in accordance with its concept of warfare, which envisions the coordinated use of military and non-military elements of national power to shape the strategic environment. Throughout Europe, Russia exercises malign influence to disrupt and attempt to fracture NATO, undermine trans-Atlantic cohesion, and erode democratic foundations. Russia interferes in the electoral process across numerous states, including supporting a plan to violently disrupt elections in Montenegro, the newest member of NATO. Russia works to influence the geopolitical environment through the use of key acquisitions, proxies, and other agents of influence. Using indirect action, particularly against countries along its periphery, Russia seeks to use information operations

As evidence collected by the transatlantic communities’ intelligence services on Russian cyber and political influence operations continues to accumulate and experts like Supreme Commander Scaparrotti share their assessments on Russian cyber operations, the purpose behind Russia’s cyber operations become increasingly irrefutable.
Chapter Six: Quantifying the Effects

This chapter focuses on available public data, primarily in the form of international polling and survey data, to answer the question first posed in Chapter One, “What were the effects of attempts by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?” Here I compare the quantitative data collected from “consolidated democracies”\(^{178}\) which were targeted by cyber operations directed against elections described in a Senate Committee on Foreign Relations report\(^{179}\) with the data collected for a control group of consolidated democracies which have not experienced similar cyber operations in order to assess the effects of cyber acts.

The data primarily used in the quantitative analysis was collected by *Gallup World Poll* which conducts annual phone and in-person interviews in over 160 countries with an average of 1,000 participants to track national perceptions on both domestic and international issues.\(^{180}\) I selected the polling questions, “In this country, do you have confidence in the national government?” and “In this country, do you have confidence in the honesty of elections?” to serve as indicators of the potential effects of cyber

\(^{178}\) The countries in this chapter are defined as “consolidated democracies,” a term taken from the Freedom House “Freedom in the World 2018: Democracy in Crisis”, which ranks and measures the progress toward or backsliding from democracy. The ranking is determined by an assessment of a country’s national democratic governance, electoral process, civil society, independent media, local democratic governance, judicial framework and independence, and corruption. Countries receiving the consolidated democracy classification are defined as ones that “embody the best policies and practices of liberal democracy but may face challenges—often associated with corruption—that contribute to a slightly lower score.” Freedom House, “Freedom in the World 2018: Democracy in Crisis.”


operations. These particular questions were selected because if the objective behind cyber operations was to increase hyper-partisanship and erode the legitimacy of democratically-elected leaders then changes in the populations’ response to these questions could demonstrate the effect of the operations.

The consolidated democracies which endured the most prolific cyber operations directed at their elections as described again in the Senate Committee on Foreign Relations report were the Netherlands, France, Germany and Italy. The United States has also been added to this test group since it has similarly been targeted by cyber operations as established in other various Senate reports. The control group, composed of consolidated democracies in which there is scant evidence of cyber operations against their elections, includes Ireland, Iceland, Canada, Portugal and Luxembourg. By comparing the data between the test group and control group, it will be possible to observe emerging trends within the data. Polling data gathered from 2008 was chosen as a base year for comparison purposes because none of the countries which endured cyber operations against their elections had yet to report evidence of active cyber operations. Likewise, polling data collected from 2016 was chosen for comparison against the base year because, as noted in the Senate Committee on Foreign Relations report and Senate Select Committee on Intelligence report, all of the countries in the test group alleged active cyber operations targeting their elections during the given year.

---


The control group, Ireland, Iceland, Canada, Portugal and Luxembourg, were selected because they all fall within the criteria of consolidated democracies and little to no evidence of active cyber operations against their national elections has yet to emerge. By taking the individual country’s responses to the polling questions and calculating the control group’s mean number for each potential response, ‘confidence,’ ‘no confidence’ and ‘unsure confidence,’ an average response for the control group is established. In 2008, when asked “In this country, do you have confidence in the national government?”, the control group’s mean numbers showed 50.4% of respondents expressed ‘confidence’ in the national government, 43% of respondents expressed ‘no confidence’ in the national government and 6.4% of respondents expressed ‘unsure confidence’ in the national government. The control group’s mean numbers for the second question, “In this country, do you have confidence in the honesty of elections?” in the same given year indicated 72.2% of respondents expressing ‘confidence’ in the honesty of elections, 22.6% of respondents expressing ‘no confidence’ in the honesty of elections and 5.4% of respondents expressing ‘unsure confidence’ in the honesty of elections. Against these base numbers we will compare the mean numbers for the control group eight years later.

The control group’s mean number, or average responses to the survey questions, showed little change from the findings of 2008 responses and what was found in the 2016 responses. For the question regarding confidence in national government 56.6% of respondents expressed ‘confidence,’ 39.8% of respondents expressed ‘no confidence,’ and 3.4% of respondents expressed ‘unsure confidence.’ For the question on confidence in the honesty of elections, there were also only small changes with 71.8% of respondents expressing ‘confidence,’ 25.8% of respondents expressing ‘no confidence,’ and 2.2% of
respondents expressing ‘unsure confidence.’ That represents an average increase in the control group’s confidence in their respective national governments by 6.2% and an average decrease in the control group’s lack of confidence by 3.2%. The change in the control group’s confidence in the honesty of elections was negligible at -.4% of respondents while those who lack confidence rose just 3.2%. All together the changes seen between 2008 and 2016 in the control group’s confidence in their national governments and the honesty of their elections were moderately small.
The polling data from the control group of consolidated democracies is displayed here:\textsuperscript{183,184}

<table>
<thead>
<tr>
<th>Country/Year</th>
<th>Control Group</th>
<th>Confidence</th>
<th>No Confidence</th>
<th>Unsure Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ireland</strong></td>
<td>2008 Confidence in National Government</td>
<td>51%</td>
<td>47%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>57%</td>
<td>38%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>70%</td>
<td>28%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>71%</td>
<td>26%</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Iceland</strong></td>
<td>2008 Confidence in National Government</td>
<td>26%</td>
<td>66%</td>
<td>8%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>61%</td>
<td>36%</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>84%</td>
<td>13%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>87%</td>
<td>12%</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Canada</strong></td>
<td>2008 Confidence in National Government</td>
<td>59%</td>
<td>39%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>62%</td>
<td>38%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>67%</td>
<td>31%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>69%</td>
<td>30%</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Portugal</strong></td>
<td>2008 Confidence in National Government</td>
<td>34%</td>
<td>49%</td>
<td>17%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>35%</td>
<td>57%</td>
<td>8%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>61%</td>
<td>25%</td>
<td>14%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>56%</td>
<td>40%</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Luxembourg</strong></td>
<td>2008 Confidence in National Government</td>
<td>82%</td>
<td>14%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>68%</td>
<td>30%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>79%</td>
<td>16%</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>76%</td>
<td>21%</td>
<td>3%</td>
</tr>
</tbody>
</table>

The test group of consolidated democracies saw a more dramatic change over the same timeframe. After collecting the individual country’s responses to the polling questions and calculating the test group’s mean numbers for each potential response, ‘confidence,’ ‘no confidence’ and ‘unsure confidence,’ we can draw comparisons between the test group’s 2008 and 2016 responses. In 2008, when asked “In this country, do you have confidence in the national government?”, the test group’s mean numbers showed 44.8% of respondents expressed ‘confidence’ in the national government, 49% of respondents expressed ‘no confidence’ in the national government and 6.8% of respondents expressed ‘unsure confidence’ in the national government. The mean numbers for the second question, “In this country, do you have confidence in the honesty of elections?” in the same year, showed 59.8% of respondents expressing ‘confidence’ in the honesty of elections, 36% of respondents expressing ‘no confidence’ in the honesty of elections and 4.6% of respondents expressing ‘unsure confidence’ in the honesty of elections. Against these base numbers we can compare the mean numbers for the test group’s data from eight years later.

The test group’s mean numbers had changed more substantially in the 2016 responses. For the question regarding confidence in national government 38.8% of respondents expressed ‘confidence,’ 59.8% of respondents expressed ‘no confidence,’ and 1.2% of respondents expressed ‘unsure confidence.’ For the question focused on confidence in the honesty of elections, there were noticeable changes as well with 52.4% of respondents expressing ‘confidence,’ 46% of respondents expressing ‘no confidence,’ and 1.4% of respondents expressing ‘unsure confidence.’ That represents an average decrease in the test group’s confidence in their national governments by 6% and an
average increase in the test group’s lack of confidence in their national governments by 10.8%. The change in the test group’s confidence in the honesty of elections was also more dramatic, decreasing by 7.4% while those who lack confidence rose by 10%. Taken together the changes seen between 2008 and 2016 in the test group’s confidence in their national governments and the honesty of their elections was fairly significant.
The polling data from the test group of consolidated democracies is displayed here:\textsuperscript{185}186

<table>
<thead>
<tr>
<th>Country/Year</th>
<th>Test Group</th>
<th>Confidence</th>
<th>No Confidence</th>
<th>Unsure Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>2008 Confidence in National Government</td>
<td>38%</td>
<td>62%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>30%</td>
<td>69%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>47%</td>
<td>53%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>30%</td>
<td>69%</td>
<td>1%</td>
</tr>
<tr>
<td>Italy</td>
<td>2008 Confidence in National Government</td>
<td>36%</td>
<td>49%</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>24%</td>
<td>75%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>52%</td>
<td>35%</td>
<td>14%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>35%</td>
<td>63%</td>
<td>1%</td>
</tr>
<tr>
<td>Germany</td>
<td>2008 Confidence in National Government</td>
<td>43%</td>
<td>51%</td>
<td>6%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>55%</td>
<td>43%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>49%</td>
<td>47%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>71%</td>
<td>27%</td>
<td>2%</td>
</tr>
<tr>
<td>France</td>
<td>2008 Confidence in National Government</td>
<td>45%</td>
<td>49%</td>
<td>6%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>28%</td>
<td>70%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>66%</td>
<td>31%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>52%</td>
<td>46%</td>
<td>2%</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>2008 Confidence in National Government</td>
<td>62%</td>
<td>34%</td>
<td>6%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in National Government</td>
<td>57%</td>
<td>42%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2008 Confidence in Honesty of Election</td>
<td>85%</td>
<td>14%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>2016 Confidence in Honesty of Election</td>
<td>74%</td>
<td>25%</td>
<td>1%</td>
</tr>
</tbody>
</table>

It’s important to establish that it would be unwise to draw any direct correlations between this analysis of changing perspectives of national governments and honesty in elections and Russian cyber operations against elections. While there are too many


country-specific political caveats to establish a correlation, the analysis does show trends that support the argument that cyber operations are having an effect on elections.

Findings from the control group appear to indicate a growing confidence in the respondents’ national governments and a small decline in those who lacked of confidence in them. Simultaneously, the control group saw only a slight decrease in their confidence in the honesty of their elections and a small increase in the number of respondents expressing a lack of confidence.

By comparison, the test group’s confidence in national elections actually declined a moderate amount while those with a lack of confidence in the national government increases substantially. Most significant was the decline in the test groups confidence in elections and their increase in respondents with no confidence in the honestly of elections, both of which saw substantial increases. The trend in this data is clear, between 2008 and 2016 the control group saw slight increase in its confidence in national governments while its confidence in the honesty of elections declined only marginally.

As for the test group, it saw both moderate decreases in its confidence in national
governments and its confidence in the honesty of elections. The test group’s trends
between 2008 and 2016 are straightforward and support (but cannot definitively be
proven) the argument that cyber operations are having a disruptive or influential effect on
the electoral process in democratic states.

The trends indicated from the analysis are more alarming when considered in a
broader context. A global survey which collected data from respondents in 38 countries
conducted in 2017 by Pew Research Center found that only 23% of respondents were
fully committed to representative democracy.189 Shockingly, a plurality of respondents at
47%, showed less commitment to representative democracy while indicating an openness
to other forms of governance. Alarmingly, 13% of respondents indicated a commitment
to nondemocratic forms of governance.190 While it is impossible to test the control group
against this data set as they were not all represented in the survey, we can find the mean
response from our test group. Compared to the global median, the test group’s average
response does not seem quite as shocking, it does indicate an alarming openness to
alternative forms of governance.191 This openness to alternative forms of governance is
only made more of a concern by the declining confidence in national governments and
honesty of elections trend established for the test group earlier.

189 Wike, Richard, et al. “Globally, Broad Support for Representative and Direct Democracy, but Many are
also Open to Nondemocratic Alternatives.” Pew Research Center, 16 October 2017.
http://www.pewglobal.org/2017/10/16/globally-broad-support-for-representative-and-direct-
democracy/pg_2017-10-16_global-democracy_0-01/.
190 Ibid.
191 Ibid.
Commitment to Representative Democracy

<table>
<thead>
<tr>
<th></th>
<th>Committed</th>
<th>Less Committed</th>
<th>Nondemocratic</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>40%</td>
<td>46%</td>
<td>7%</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>47%</td>
<td>37%</td>
<td>8%</td>
</tr>
<tr>
<td>Italy</td>
<td>37%</td>
<td>42%</td>
<td>9%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>36%</td>
<td>47%</td>
<td>10%</td>
</tr>
<tr>
<td>France</td>
<td>35%</td>
<td>45%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Test Group's Average</strong></td>
<td><strong>39%</strong></td>
<td><strong>43%</strong></td>
<td><strong>9%</strong></td>
</tr>
</tbody>
</table>

As disconcerting as these emerging trends are, it is also important to contextualize the results along with other quantitative findings. These indicate that the health of democracy and the electoral process remain robust. The Economist Intelligence Unit has constructed a democratic index for over 165 states, collecting data on various quantitative factors with which they calculate a measurement of democracy’s health in a nation since 2006. “The Democracy Index is based on five categories: electoral process and pluralism; civil liberties; the functioning of government; political participation; and political culture.”

When the test group and control group are tested against the Economist Intelligence Unit’s findings it helps to temper the earlier findings regarding declining confidence in national governments and honesty in elections. This can be seen by comparing the control group and the test group’s annual scores on the democratic index.

---


which indicate few discrepancies between the two groups and show little volatility since the measurement was first taken in 2006.

Test Group's Democratic Index Score:

<table>
<thead>
<tr>
<th>Year</th>
<th>United States</th>
<th>Italy</th>
<th>France</th>
<th>United Kingdom</th>
<th>Netherlands</th>
<th>Test Group's Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>8.22</td>
<td>7.73</td>
<td>8.07</td>
<td>8.08</td>
<td>9.66</td>
<td>8.352</td>
</tr>
<tr>
<td>2007</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>2008</td>
<td>8.22</td>
<td>7.98</td>
<td>8.07</td>
<td>8.15</td>
<td>9.53</td>
<td>8.39</td>
</tr>
<tr>
<td>2009</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>2010</td>
<td>8.18</td>
<td>7.83</td>
<td>7.77</td>
<td>8.16</td>
<td>8.99</td>
<td>8.186</td>
</tr>
<tr>
<td>2011</td>
<td>8.11</td>
<td>7.74</td>
<td>7.77</td>
<td>8.16</td>
<td>8.99</td>
<td>8.154</td>
</tr>
<tr>
<td>2012</td>
<td>8.11</td>
<td>7.74</td>
<td>7.88</td>
<td>8.21</td>
<td>8.99</td>
<td>8.186</td>
</tr>
<tr>
<td>2013</td>
<td>8.11</td>
<td>7.85</td>
<td>7.92</td>
<td>8.31</td>
<td>8.84</td>
<td>8.206</td>
</tr>
<tr>
<td>2014</td>
<td>8.11</td>
<td>7.85</td>
<td>8.04</td>
<td>8.31</td>
<td>8.92</td>
<td>8.246</td>
</tr>
<tr>
<td>2015</td>
<td>8.05</td>
<td>7.98</td>
<td>7.92</td>
<td>8.31</td>
<td>8.92</td>
<td>8.236</td>
</tr>
<tr>
<td>2016</td>
<td>7.98</td>
<td>7.98</td>
<td>7.92</td>
<td>8.36</td>
<td>8.8</td>
<td>8.208</td>
</tr>
<tr>
<td>2017</td>
<td>7.98</td>
<td>7.98</td>
<td>7.8</td>
<td>8.53</td>
<td>8.89</td>
<td>8.236</td>
</tr>
</tbody>
</table>

Control Group's Democratic Index Score:

<table>
<thead>
<tr>
<th>Year</th>
<th>Iceland</th>
<th>Ireland</th>
<th>Canada</th>
<th>Luxembourg</th>
<th>Portugal</th>
<th>Control Group's Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>9.71</td>
<td>9.01</td>
<td>9.07</td>
<td>9.1</td>
<td>8.16</td>
<td>9.01</td>
</tr>
<tr>
<td>2007</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>2008</td>
<td>9.65</td>
<td>9.01</td>
<td>9.07</td>
<td>9.1</td>
<td>8.05</td>
<td>8.976</td>
</tr>
<tr>
<td>2009</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>2010</td>
<td>9.65</td>
<td>8.79</td>
<td>9.08</td>
<td>8.88</td>
<td>8.02</td>
<td>8.884</td>
</tr>
<tr>
<td>2011</td>
<td>9.65</td>
<td>8.56</td>
<td>9.08</td>
<td>8.88</td>
<td>7.81</td>
<td>8.796</td>
</tr>
<tr>
<td>2012</td>
<td>9.65</td>
<td>8.56</td>
<td>9.08</td>
<td>8.88</td>
<td>7.92</td>
<td>8.818</td>
</tr>
<tr>
<td>2013</td>
<td>9.65</td>
<td>8.68</td>
<td>9.08</td>
<td>8.88</td>
<td>7.65</td>
<td>8.788</td>
</tr>
<tr>
<td>2014</td>
<td>9.58</td>
<td>8.72</td>
<td>9.08</td>
<td>8.88</td>
<td>7.79</td>
<td>8.81</td>
</tr>
<tr>
<td>2015</td>
<td>9.58</td>
<td>8.85</td>
<td>9.08</td>
<td>8.88</td>
<td>7.79</td>
<td>8.836</td>
</tr>
<tr>
<td>2016</td>
<td>9.5</td>
<td>9.15</td>
<td>9.15</td>
<td>8.81</td>
<td>7.86</td>
<td>8.894</td>
</tr>
<tr>
<td>2017</td>
<td>9.58</td>
<td>9.15</td>
<td>9.15</td>
<td>8.81</td>
<td>7.84</td>
<td>8.906</td>
</tr>
</tbody>
</table>

* Data for a given year is unavailable.
195 Ibid.
Viewing the data comprehensively, there are a few findings that stand out most clearly. Compared against the control group, the test group of consolidated democracies displayed declining confidence in both their national governments and the honesty of their elections. While one cannot directly assert a correlation between Russia’s use of cyber operations against elections and these findings they do establish an alarming trend. Furthermore, a plurality of respondents from our test group are, at least in surveys, open to other forms of governance besides representative democracy while a sizable minority are even open to nondemocratic forms of governance. This aspect is crucial as it indicates if the trends of decreasing confidence in national governments and honesty of elections are not reversed, there are significant portions of society within the test group countries that would be open to alternative forms of governance. As disturbing as these trends appear, by other measures democratic and electoral health remain strong. Considering the implications that both the test and control groups have maintained strong scores on the democratic index for over a decade, the health of the democratic and electoral institutions does not seem to be a concern. Rather, the findings are indicative of the electorate which is made up of people and if people increasingly perceive these institutions with diminished confidence it could undermine the system as a whole.

See Annex A for graphic representation of each individual country’s annual confidence in their national government and confidence in the honesty of their elections.
Chapter Seven: Russia’s International Meddling and Active Measures – An
Interview with a Former Eastern European Official

This study has established in previous chapters that cyber operations are just one type of active measure Russia has employed to accomplish its strategic goal of countering and degrading the Euro-Atlantic regional security framework provided by the European Union and NATO. These efforts are ongoing and multipronged. While government officials and the media in Western Europe and North America are only starting to become aware of these Russian objectives, many in Eastern Europe have experienced first-hand what Russian active measures can accomplish when not sufficiently confronted. This chapter offers insight into Russian active measures witnessed and experienced by a former government official from Moldova. The former official, Vladimir Lupan, has held numerous high-level government positions in which he has witnessed with rising alarm Russia’s growing influence and the corrosive effects of its active measures on regional domestic politics.

In order to appreciate Mr. Lupan’s account, we must first contextualize Moldova geographically, historically and geopolitically. Given Moldova’s relatively low international profile, its place on the map remains obscure to many. Moldova, a former Soviet republic, is an Eastern European country wedged between northeastern Romania and southwestern Ukraine which gained its independent in 1991. Its capital, Chișinău, lies in between the two rivers which dominate the country. To the west, the Prut River serves as a border with Romania, while to the east the Dniestr River and adjacent lands border Ukraine. Circumstances in the east are complicated by what many Moldovans have seen as evidence of Russia’s continued international meddling in the country. Trans-
Dniestr or Transnistria, a strip of land between Ukraine and the Dniestr River which ranges from two to 25 miles wide, is the home of a Russian-supported secessionist movement and has been a source of tension even preceding Moldova’s independence.

The roots of the division can be traced to the Soviet Union’s earliest expansionist policies. When Soviet authorities first decided to create the Moldavian Autonomous Soviet Socialist Republic (Moldavian ASSR) on March 7th, 1924, it was composed of the Transnistria region and portions of the Ukrainian Soviet Socialist Republic (Ukrainian SSR) and, though autonomous, fell under the administration of the Ukrainian SSR. Historical evidence suggests that the Moldavian ASSR (MASSR) was created by the Soviets to serve the dual purposes of bolstering Soviet claims to Bessarabia, an eastern territory of the Kingdom of Romania which bordered the newly-created MASSR, and exporting the Soviet’s ideology to Romania and the wider Balkans region. In pursuit of these goals, the Soviets directed both industrialization and Russian, Belarusian and Ukrainian immigration to the region. In 1939, as a stipulation of the Molotov-Ribbentrop Pact, Nazi Germany recognized Soviet sovereignty in Bessarabia which led to Romania relinquishing the territory and its incorporation into the newly-formed Moldavian Soviet Socialist Republic (Moldavian SSR) in 1940. During WWII, with German military assistance the Romanians gained control of the Moldavian SSR briefly but it was recaptured by the Soviets in 1944. For clarity, Bessarabia, formerly part of the

198 Ibid.
200 Ibid.
Kingdom of Romanian, comprises the western portion of modern day Moldova together with Transnistria to east.

In the aftermath of the war, the Moldavian SSR was reinstated. Soviet immigration and development patterns established before the war, strengthened by Soviet suspicion of ethnic Moldavians’ loyalty to the USSR, led to a reemergence of industrialization policy which was preferential to Transnistria at the expense of the rest of the Moldavian SSR. These patterns were self-perpetuating as a lack of development led to resentment among the ethnic Moldavians in the west and as job opportunities drew ethnic Russians, Belarusians and Ukrainians to Transnistria which in turn spurred greater investment in the territory. As the USSR was dissolving, these patterns had created pronounced ethnic distinctions and immense disparities in industrial capacity between Transnistria and the rest of Moldavia.

These regional ethnic and industrial discrepancies within Moldovia, led to societal cleavages that erupted into violence before the country had even declared independence in 1991. By September, 1989, Tiraspol which served as Transnistria’s de facto capital, was demanding protections for minority languages and to preserve the region’s political clout. As the USSR demise appeared increasingly inevitable, many ethnic Russians, Belarusians and Ukrainians in Transnistria took the preemptive step of declaring

---

203 Ibid.
Transnistrian independence, establishing what they called the Pridnestrovian Moldavian Republic, out of fear of Moldova’s potential reunification with Romania. This move quickly led to conflict. Between November 1990 and July 1992, Transnistrian separatists, with alleged support from the Russian 14th Army regiment stationed within the region, fought the newly-formed Moldavian military forces to a cease fire. In the aftermath of the conflict, Russia maintained a military presence in the region and offered its support for Tiraspol both politically and economically.

While support for Transnistria represents Russia’s most overt example of interfering in Moldova’s domestic politics, in many ways, it served only as the entry point for Russian covert efforts at interference within the country. Since Moldova declared independence on August 27th, 1991, Moscow has used negotiations with the breakaway region and the issue of protecting the rights of ethnic Russians as a way to involve itself in Moldovan affairs. As established in the 1994 Constitution, the country adopted a democratic, unicameral parliamentary republic and saw a democratic and centrist agrarian party win a plurality of parliamentary seats in the country’s first election held same year. These early years saw the country’s state-directed economy transition to a market-based economy which caused economic pain and resulted in declining and dismal GDP growth that continued until 1999. Economic headwinds as well as

---

208 Ibid.
210 Ibid.
nostalgia for the relative calm of the Soviet era provided potent campaign issues and secured an electoral plurality for the Party of Communists in the 1998 election.\textsuperscript{212} The remaining vote was divided between three pro-democratic parties, all of which were advocating greater integration with Western Europe, while the agrarian party which held power was stripped of all representation.\textsuperscript{213} The Party of Communists, difficult to place on a traditional ideological spectrum, held deeply conservative social views and advocated for greater ties with Russia, while nominally promoting a left-leaning economic platform.\textsuperscript{214} A similar pattern continues to the modern day, with the government switching hands between a communist party in support of greater ties to Russia and a coalition of liberal and centrist parties in support of greater ties to the European Union.\textsuperscript{215} Those who support greater integration with the EU, would argue that whenever they made significant steps towards their goal, Russian domestic interference became more pronounced.\textsuperscript{216}

While this summation could not possibly capture all the subtleties of Moldovan domestic politics or its historic relations with Russia or Western Europe, it should provide enough background to contextualize the proceeding interview with Vladimir Lupan. Mr. Lupan has had a distinguished career, serving as a member of the Moldovan Parliament, during which time he served on the Committee on National Security, Defense and Public Order and as an alternate member on its Committee on Foreign Affairs and

\textsuperscript{213} Ibid.
European Integration.\textsuperscript{217} In addition, Mr. Lupan has served as Foreign Policy Adviser to the Acting President of the Republic of Moldova and held numerous diplomatic posts including Ambassador & Permanent Representative of the Republic of Moldova to the United Nations, Head of Political-Military Cooperation with the NATO and a member of the Organization for Security and Cooperation in Europe (OSCE) Mission to Croatia.\textsuperscript{218}

Over the course of his career, he has advocated for greater cooperation between Moldova and the European Union, opposed increasing ties to the Russian Federation and loudly objected to Russia’s incursion within Moldovan politics. In expressing these positions, Mr. Lupan has himself become the target of a disinformation operation. He now resides in New York, working as an independent expert in international affairs, where he was gracious enough to share his thoughts on Russia’s international meddling and active measures. As the interview was extensive, in order to ensure clarity and concision portions specifically relevant to Russian cyber operations and active measures are presented here. The interview in its entirety can be found in Annex B.

Interviewer: How would you describe relations between Russia and Moldova since Moldova signed the Association Agreement with the European Union in 2014? Can you elaborate on any role Russia may have in Moldova’s domestic politics with regards to the breakaway region of Transnistria?


\textsuperscript{218} Ibid.
Vladimir: In 1998, there was even a partnership agreement with the EU and we began negotiating the partnership agreement in 1994 and it was agreed to in 1998. In 1999-2000 there was an agreement to upgrade the partnership. Moldova only became independent in 1991 and started negotiating with the EU in 1994 so it was only three years. Moldova has a history of moving towards the EU, practically from its independence but Russia showed its true face with the Kozak Memorandum. What was the purpose of this exclusive veto power for the separatists? It is to give them autonomy and Russia has influence over this faction. It’s is purely an attempt to grant them leverage over Moldova. They would have the power in the decision process, we called this the Transnistria-ization of Moldova. Later, you also saw the Transnistria-ization of Ukraine and the developments were essentially the same. This process involves federalization which sounds good but the plan was written by Russia in such a manner to give a small actor veto power over the larger actor be it Moldova or Ukraine while Russia maintains influence over that small minority. You can even see these same tactics being applied in the United States, it’s a different matter but during the 2016 elections there were numerous succession groups in the United States that were supported by Russia. In this way Moldova is a testing ground. However, in 2013, in Moldova you saw a backlash both internally and externally which caused the Party of Communists to reject the Kozak Memorandum and Russia responded harshly with the embargo of wines and manipulation of energy,
in the form of gas, prices. It was a form of punishment. You could see Germany paying less for gas than Moldova even though it is farther from Russia. The EU does not act with a single voice so it’s much easier to attempt to divide and conquer the member states. It’s worth remembering that Vladimir Putin was the head of the KGB an organization that had worked on dividing and conquering Europe for years.

Interviewer: You’ve called Moldova a testing ground for Russian political interference on Twitter and in response to the Russian disinfection campaigns in July, 2017, the Moldovan Parliament finally adopted an Anti-Propaganda Law. Can you explain what prompted the law, how it was justified and received domestically and if you believe it’s proving effective?

Vladimir: When I say Moldova is a “testing ground” you have to understand that I’m referring to the use of proxies, and by proxy, I mean a military that will do the dirty work without wearing your insignia. This concept is equally applicable in all Russia’s efforts and not necessarily only military. Try to be more flexible in your thinking. Whatever means Russia can find in a country to use it against that country, if it is a political party or a paramilitary, if it’s a struggling population longing for some specific relation or benefits from Russia then they will become a paramilitary, if there is a hacker who is interested in making the government pay a price, for example Edward Snowden and the U.S., then
they will use that against the country. They will use Wikileaks to release
documents or when possible, they will use their own “patriotic” hackers to
release any data when possible.

Interviewer: Pro-Russian media in Moldova have been spreading
news of the imminent restitution of historical land and property held by
Ukrainian citizens to Poland and likewise Moldovans having to return land
and property to Romania. According to these fake reports, the Association
Agreements that both Ukraine and Moldova signed with the European
Union in 2014 calls for such restitution. The Association Agreement calls
for nothing of this sort. What effects have such online “fake news” sources
had on Moldova and how can “fake news” propagated online be
neutralized?

Vladimir: It’s funny you mention this. These stories of Moldova
having to give territory back to Romania. Here in New York, I was sitting
with my Russian barber and he asked me about this very issue. He asked
me why Moldovans would accept giving up territory in order to join the
European Union. I asked him where he had heard this and he pointed to
his television. It was on Russia-1 [a state-sponsored, Russian language
channel carried internationally]. I told him it wasn’t the case which he had
trouble believing. This is occurring all the time and because there are few
channels here in Russian many Russians who live abroad see these types
of reports. They have an effect. There is disinformation but you should
look up the concept of *Whataboutism* by the journalist Michael Bernard, its similar to the *tu quoque* logical fallacy. It is a technique the Soviets used where if someone says something critical, you change the topic to something distracting and more preferable. Americans would object to a specific Soviet human rights abuse and the Soviets would counter with something like “What about racism in America?” Obviously, both aren’t good but the objective of the person using *Whataboutism* was to change the subject. How can “fake news” propagated online be neutralized? Well, as we saw, this is difficult. There can be laws but as in Moldova you have to see the details of those laws.

**Interviewer:** Russia’s foreign military intelligence agency, the Main Intelligence Directorate (GRU) and the Federal Security Services (FSB) are believed to have played a part in Russia’s interference in the 2016 US presidential election through online groups respectively known as “Fancy Bear” and “Cozy Bear” by penetrating the Democratic National Committee (DNC) in 2015 and releasing stolen and compromising information at a time when it would have the greatest political impact. Have you seen any comparable efforts in past Moldovan elections or do you suspect they could take place in next year’s parliamentary elections?

**Vladimir:** In Moldova, the tactics used by Russia are more brazen. They can use tactics they wouldn’t dare to use in the United States. Rather than covertly attempting to manipulate an election, they can afford to be
overt in their support of a party or candidates. This is combined with
disinformation against candidates who stand up to Russia or promote
deeper integration with the European Union. In this was the situation is
different between Moldova and the United States.

Interviewer: Russia has a long record of targeting outspoken critics
in an attempt to delegitimize them in the public eye. Considering your
position and outspoken criticism of Russian propaganda campaigns, have
you had any experiences with cyber intrusion or attempts to compromise
your character that you would be willing to share?

Vladimir: This occurred when I was serving as the Ambassador &
Permanent Representative of Moldova to the United Nations over the
Russian involvement in Syria. There were Russian media reports claiming
I had proposed rescinding Russia’s veto authority on the United Nations
Security Council. This is impossible. There is absolutely nothing in the
UN Charter about removing a Security Council member’s right to a veto.
There is no mechanism for that, so it would be impossible. This was about
building pressure diplomatically. Similar circumstances happened to
others at the UN over Russian involvement in eastern Ukraine. As you
know, Moldova is not on the Security Council and even if it was, there is
no way to take away a veto from a Security Council member. It fits a
pattern though, they take elements of truth, in this case, another diplomat
had proposed a resolution in which veto authority would be challenged on
a one-time issue for countries that prevented serious inquires on war crimes, crimes against humanity or genocide and shape it to their purposes.

Interviewer: What are the long-term objectives of Russia’s cyber aggression and propaganda campaigns?

Vladimir: The purpose of Russian ops is not only to deceive the West but also to destroy the values of the West. They target our collective values. They want to destroy the rule of law in these countries. They want to undermine the EU and NATO. They do this by bashing relations between countries with things like gas price manipulation and they do it within countries by bashing certain political parties. It’s about freedom to act. It’s about realpolitik, when certain national security issues are present, Russia understands realpolitik well and they use the resources available. Essentially, Russia sees the United States as a country that can prohibit them, for external and internal reasons, from expanding. Therefore, any attempt by an administration to try to stop Russian actions will actually face some sort of response. In order to solve a problem, you need to have a willing partner, that’s the bilateral part of negotiations, you need to agree on a certain set of actions, up to now I have not seen Russia willing to stop. What we’ve see is Russia trying to restore its status as a superpower, which they are incapable of. They are a regional power but not a superpower, they cannot do more than that.
After discussing Russia’s efforts at internal interference in Moldovan politics and its use of active measures, what became clear, was the fact that Russian active measures are adaptable and different active measures are used to meet the needs of a given situation and its context. Moscow may not need to use cyber interference in Moldova because it can utilize leverage against individual politicians or even political parties. While such tactics are too transparent to be used effectively in some Western European countries and the United States, if they work within a specific context, Russia will not hesitate.

In contemplating Russia’s use of active measures, there is two commonalities that all the active measures seem to share. The first is their ability to erode a society’s commitment to the rule of law. Be it promoting the distribution of knowingly stolen emails to the electoral detriment of a political opponent or providing financial incentives to politicians to support dubious geopolitical positions. It is in this slow erosion of a country’s commitment to the rule of law, that active measures also find their second commonality which is the promotion of Russia’s long-term geopolitical objectives. This is because at the center of Russia’s geopolitical ambitions is a desire to remove the model of governance offered by nations in Western Europe and North America. Russia’s governance is built on a system of corruption and patronage, it relies on a network of oligarchs maintaining Vladimir Putin’s favor and it has no ideological underpinning. The Russian regime seeks the dissolution of the European Union and the breakup of NATO as long-term strategic goals because they stand as attractive alternatives to the Russian form of governance.
Chapter Eight: Conclusion and Recommendations

In this thesis I have attempted to answer some basic questions about the use of cyber operations as a means to disrupt, alter or influence state’s electoral processes. The research involved in answering these questions unearthed some alarming insight into the ways in which evolving technology has and likely will continue to be adopted by state intelligence agencies. These new cyber operations have expanded the efficacy and scope of intelligence agencies’ operations as well as presented the opportunity for innovative, new, covert operations to be conceived and carried out. While limitations in available data and geopolitical realities narrowed the scope of this research to a focus on, primarily, Russian cyber operations directed at state’s electoral processes, there is ample evidence to support the international community’s concern regarding Russia’s malign use of cyber operations in general.

In the introduction to this thesis, I outlined several questions which aimed to uncover the various aspects of cyber operations and their potential impact on electoral processes. After examining the research and findings, it is worthwhile to reconsider those questions:

- What is the evidence that there have been verifiable attempts by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?

Over the course of the research, numerous documented cyber investigations have emerged. These cyber investigations, conducted by independent experts and international organizations as well as the U.S. intelligence community, have asserted with high levels
of confidence that Russian state-sponsored actors have been involved in various attempts to disrupt, alter and influence state’s electoral processes.  

- What were the methods used by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?

For clarity, the methods used to disrupt, alter and influence electoral processes were organized into three types of cyber operations based on the primary target of the operation. The designated targets for each type of those cyber operations were the voting equipment and election infrastructure, the elected officials, political operatives and political parties and the broader public. Evidence uncovered by the FBI’s Cyber Division demonstrates the depth and scope of Russia’s cyber operations that penetrated U.S. state’s voting registries and electoral boards.  

Independent cyber investigations led by the industry’s leading firms SecureWorks and TrendMicro have traced the most notorious examples of cyber operations against political campaigns, the Clinton and Macron presidential campaigns, back to Russian IP addresses. Cyber operations conducted by Russian state-sponsored actors against the public, primarily through social media

---

Platforms such as Facebook and Twitter, have been exposed by the independent media and confirmed by various intelligence services as well as the corporate leadership within the social media platforms.224

These new types of cyber operations are an outgrowth of intelligence services adapting to emerging technologies. Russian intelligence agencies have a long history of leveraging any advantage and utilizing rival nation’s societal division to advance Russia’s geopolitical goals. These technological advances made many existing active measures, such as the dispersion of propaganda and disinformation, media manipulation, malign political influence, deception, the funding of extremist and opposition groups, spreading conspiracy theories and rumor, and espionage, immeasurably more effective.228

By complementing existing Russian intelligence agencies’ active measures with cyber operations, these agencies were able to use active measures in innovative, while still untested, new ways to target numerous state electoral processes at a relatively low risk and cost.

---

What were the effects of attempts by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated cyber operations?

Unfortunately, the answer to any question posed regarding the effects of cyber operations, or attempted cyber operations, on state electoral processes remains elusive and intensely contentious. While this thesis has provided both quantitative and qualitative data which point to the corrosive effects of cyber operations on state electoral processes, it cannot conclusively determine the effects. That being established, the data collected is somewhat persuasive in making the case that cyber operations are having a deleterious effect on electoral processes.

By comparing “consolidated democracies” targeted by cyber operations against the data collected for a control group which had not experienced similar cyber operations, some alarming trends were uncovered. The test group of consolidated democracies experiencing attacks saw an average decrease in the group’s confidence in their national governments by 6% and an average increase in the group’s lack of confidence in their national governments by 10.8% during a period when Russia intelligence services were most active. Similarly, the group’s average confidence in the honesty of elections also saw dramatic changes, decreasing by 7.4%, while those who lack confidence rose by 10% over the same period. These trends only appeared more alarming when compared against

229 The countries in this chapter are defined as “consolidated democracies,” a term taken from the Freedom House “Freedom in the World 2018: Democracy in Crisis”, which ranks and measures the progress toward or backsliding from democracy. The ranking is determined by an assessment of a country’s national democratic governance, electoral process, civil society, independent media, local democratic governance, judicial framework and independence, and corruption. Countries receiving the consolidated democracy classification are defined as ones that “embody the best policies and practices of liberal democracy but may face challenges—often associated with corruption—that contribute to a slightly lower score.” Freedom House, “Freedom in the World 2018: Democracy in Crisis.”
a control group of democracies which had not been targeted by extensive Russian cyber operations nor seen similar negative trends in public sentiment over the same period. The findings appear to suggest that in targeted consolidated democracies, Russian cyber operations were in fact having a corrosive effect on the public’s confidence in both the honesty of elections and their national governments.

While the polling data established aggregate international trends which are noteworthy, the interview with former Ambassador & Permanent Representative of the Republic of Moldova to the United Nations, Vladimir Lupan, provided a more nuanced analysis of the long-term effects of unchecked Russian active measures and cyber operations. By Mr. Lupan’s telling, Russian intelligence agencies are actively pursuing the dissolution of the European Union and NATO and will use any and all methods that prove effective. His account outlined the various ways in which the Russian state attempts to coerce and manipulate smaller states through its energy and trade policy as well as directly supporting candidates, parties and factions within a state’s domestic politics. Mr. Lupan expressed grave concern over the lack of a unified, forceful response to Russian interference in state’s domestic politics and its pronounced disinformation campaigns. One of the key insights, however alarming, was Mr. Lupan’s assessment that Russian intelligence services will never be satisfied, rather they will continue to interfere in state’s domestic politics through cyber operations and any other means available until confronted.

One question, not previously considered in this thesis, concerns what can be done to mitigate the effects of attempts by states, state-directed actors, or non-state actors to disrupt, alter or influence the electoral process in democratic states through coordinated
cyber operations. Fortunately, various governments currently combating these issues, in coordination with cyber security firms and international organizations, have already begun the work necessary to counter and expose Russian intelligence services ongoing cyber operations. While the countermeasures that have been taken are a response to Russian cyber operations, they offer solutions that may be applicable against cyber operations more broadly.

The most widely emphasized guidance with regards to mitigating Russian disinformation and “Fake News” more generally, has been to increase the public’s awareness of the issue and its ability to think critically when considering sources of information. There are valuable lessons to be learned from the Baltic and Scandinavian nations which never saw the threat of Russian active measures completely disappear after the fall of the Soviet Union. Sweden, for example, has plans to implement a nationwide primary school programs to help students identify Russian propaganda.\(^\text{230}\) The program, which is scheduled to begin in July 2018, aims to increase student’s digital competence and increase their ability to differentiate between reliable and unreliable sources.\(^\text{231}\) This initiative was spurred on by national polling data which indicated that eight out of ten Swedes believed disinformation was having an impact on their perceptions of basic facts.\(^\text{232}\) Sweden is not alone in using the education system to bolster its resilience to the spread of disinformation. Holland and Finland have also set strong examples to follow.


\(^\text{232}\) Ibid.
while countries in southern Europe, like Italy, are experimenting with their own programs. As the issue has become more prevalent, educational initiatives are gaining traction across Europe and the U.S. as NGOs and international advocates see their potential to blunt the effects of disinformation.

Yet, systemic changes to national education systems are often slow processes which may not help to mitigate the spread of disinformation in the near-term. Due to these concerns, experts are also advocating for greater public awareness of the issue. Jed Willard, Director of the Harvard University-based FDR Center for Global Engagement offers very specific advice to craft a unified, national, public message which can serve as an alternative to disinformation narrative. Where Russian disinformation frequently employs negative and racialized messages meant to fray societal cohesion, Willard advises promoting a positive narrative which has broad appeal across the national political spectrum.

Jed Willard, who has advised both the Swedish and Finnish governments on these issues is wary of legislation which could restrict freedom of speech and could potentially be against those attempting to mitigate Russian disinformation. Adam Berinsky, a

238 Ibid.
Professor of Political Science at the Massachusetts Institute of Technology (MIT) shared this assessment, emphasizing that members of the media and government officials should resist correcting Russian disinformation and instead highlight a positive national narrative.\textsuperscript{240} While many of these public awareness campaigns are still in development, there have been positive signs they are beginning to have an effect. For example, in Lithuania, citizens have begun volunteering their time to establish cyber-monitoring teams which have been identifying Russian-sponsored socialbots, content and Russian trolls presenting themselves as Lithuanians. Light-heartedly considering the fact that they battle Russian “Trolls” in cyberspace, they call themselves “Elves.”

Beyond building greater resistance to Russian disinformation campaigns, many security experts across the Transatlantic community have been advocating greater coordination in approach and information sharing among allies. In the wake of Russia’s cyber operation on the 2016 U.S. presidential election, the European Commission’s European Political Strategy Centre issued a report calling for the creation of a “European Cyber Shield.”\textsuperscript{241} It envisioned a comprehensive cyber security defense strategy that would cover all member states and emphasize the protection of crucial industries such as communications, healthcare, security, energy, financial services, and IT services, as well as democratic institutions.\textsuperscript{242} The report noted the current fractured state of the EU’s cyber security and foresaw the need for greater international cooperation in the fields of cyber security.

\textsuperscript{242} Ibid.
both IT security and intelligence.\textsuperscript{243} Enhancing cyber security cooperation and committing to the implementation of a EU-wide cyber security strategy should be among Europe’s top priorities.

NATO appears to have learned the risks associated with Russia’s cyber operations earlier than the EU, but it too must reevaluate its cyber security apparatus and make greater efforts to build a comprehensive cyber defense that can protect all of its members. Following a trivial dispute between Estonia and Russia in 2007, Estonia was hit with a debilitating cyber-attack against governmental, financial and communications infrastructure which was widely attributed to Russia.\textsuperscript{244} Following this clear provocation, NATO issued its first Cyber Defense Policy in 2008.\textsuperscript{245} Yet, NATO remained largely reactionary, only calling for a Cyber Defense Pledge, under which all members were to make enhanced cyber resiliency a matter of priority, and sign the Technical Arrangement of Cyber Defense with the EU in 2016. While NATO and the EU officials have made joint declarations in which they have pledged greater cooperation on cyber security, concrete action must happen faster if it is to counteract Russian growing cyber operations. In addition to removing the institutional barriers to greater cyber cooperation, the EU and NATO should support and learn from the proactive cyber defense models for

\begin{itemize}
\end{itemize}
combating Russian cyber operations that are being implemented in Scandinavia and the Baltics.\textsuperscript{246}

Unfortunately, considering the insight offered in a previous chapter from Vladimir Lupan, simply fortifying the West’s cyber security infrastructure and its public’s resistance to disinformation is unlikely to deter future Russian cyber operations. With the material costs associated with conducting cyber operations low and relatively few external disincentives placed on Russia for its operations, Russia continues to see cyber operations as a cost-effective method to undermine Western institutions. Only when the cost of Russia’s actions is considered greater than the potential benefits of its cyber operations will it be convinced to stop. Considering this insight, policymakers across the transatlantic community should turn to asymmetric forms of retaliation to counter Russian cyber aggression.

There are numerous ways in which the transatlantic community could strike back against Russian cyber operations which exclude traditional kinetic force. Perhaps the most irritating to Vladimir Putin would be supporting democratic institutions and processes within Russia itself. This could include offering funding to the few remaining NGOs and independent media outlets still operating within Russia. It could not be done covertly, as such actions would likely be perceived as interfering in the country’s domestic politics, but rather overtly and in support of values enshrined in the Helsinki Final Act to which Russia is a signatory. American and European intelligence services should be recruited in this effort, to reveal verified corruption among Russia’s

intelligence services and oligarchs. To this end, the intelligence services could work to expose any corruption associated with energy or trade policy as well as alleged Russian assassination attempts, malign influence strategies and disinformation campaigns. Again, these efforts would need to be overt and verifiable as to not be perceived as an attempt at internal meddling in another country’s domestic politics.

Thanks to U.S. and European dominance in the international financial sector, the transatlantic community has one very large asymmetric target to leverage against Russia. American and EU financial regulators should work in coordination to expose and freeze all Kremlin-linked money associated with organized crime and covert international political patronage. Further, the U.S. Treasury Department and the European Central Bank should work in concert to further identify and penalize the oligarchs who support Vladimir Putin’s regime and enable his foreign adventurism. This could include the freezing of internationally held assets and issuing personal travel restrictions to oligarchs as a means of isolating those who enable Putin’s maligning agenda.

In this thesis, I have attempted to answer some of the most preliminary questions surrounding cyber operations and the impact they can have on electoral processes. In the course of the research, it became apparent that cyber operations are a broad category in which hackers and cyber security experts are continuously innovating. Many of these individual types of cyber operations certainly warrant further research. Alarmingly, the research has shown that cyber operations, even unsuccessful operations, are likely to have an impact on public perceptions of elections. Given the covert nature of cyber operations, I suspect additional details will inevitably emerge which provide greater insight on the precise impact cyber operations have on electoral processes, but as of this writing, that
precise impact remains elusive. As the threat associated with cyber operations becomes increasingly pervasive, it is heartening to see greater acknowledgement and collaboration across the fields of academia, cyber security and national defense to address this threat.
Bibliography

https://archive.org/details/TheSwordAndTheShield-TheMitrokhinArchiveAndTheSecretHistoryOfTheKGB.

www.facebook.com/KindredOnline/posts/10152883456259681.


“СБУ ліквідувала вірус, що мав знищити результати виборів (The SBU Eliminated a Virus that was Supposed to Destroy Election Results).” *Українська правда (Ukrainian Pravda)*, 23 May 2014. 


Cox, Ana Marie. “Making Mischief on the Web.” *Time Magazine*, 16 December 2006. [http://content.time.com/content/time/magazine/article/0,9171,1570701,00.html](http://content.time.com/content/time/magazine/article/0,9171,1570701,00.html).


Khalaf, Roula. “Taking the Fight Against Fake News to the Classroom.” *Financial Times*, 22 March 2017. [www.ft.com/content/218bc046-0e69-11e7-a88c-50ba212dce4d](http://www.ft.com/content/218bc046-0e69-11e7-a88c-50ba212dce4d).


Priest, Dana, and Michael Birnbaum. “Europe Has Been Working to Expose Russian Meddling for Years.” *Washington Post*, 25 June 2017. [www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russian-meddling-for-years/2017/06/25/e42dcece-4a09-11e7-9669-250d0b15f83b_story.html?noredirect=on&utm_term=.a4c676c6933c](http://www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russian-meddling-for-years/2017/06/25/e42dcece-4a09-11e7-9669-250d0b15f83b_story.html?noredirect=on&utm_term=.a4c676c6933c).


U.S. Senate. Select Committee on Intelligence. Statement of Thomas Rid, Professor, Department of War Studies, King’s College London, Disinformation: A Primer in Russian Active Measures and Influence Campaigns. Testimony. 30 March 2017. 115th Cong. 1st sess.

108


Annex A

Additional information relevant to Chapter Six: Quantifying the Effects. Graphic representation of control group’s changing perceptions:

Irish Confidence in National Government

Irish Confidence in Elections
Icelandic Confidence in National Government

Icelandic Confidence in Elections
Luxembourgian Confidence in National Government

Confidence: 82%, 77%, 77%, 74%, 74%, 66%, 69%, 68%, 74%
No Confidence: 14%, 20%, 18%, 19%, 21%, 30%, 28%, 30%, 23%
Unsure Confidence: 4%, 3%, 5%, 7%, 4%, 3%, 2%, 3%, 4%

Luxembourgian Confidence in Elections

Confidence: 79%, 74%, 78%, 79%, 76%, 77%, 80%, 76%, 78%
No Confidence: 16%, 22%, 16%, 17%, 18%, 21%, 19%, 21%, 18%
Unsure Confidence: 5%, 3%, 5%, 3%, 6%, 2%, 1%, 3%, 4%
Graphic representation of test group’s changing perceptions:

American Confidence in National Government

American Confidence in Elections
Italian Confidence in National Government

Italian Confidence in Elections

Annex B

From Chapter Seven: Russia’s International Meddling and Active Measures - An Interview with a Former Eastern European Official. Interview with Vladimir Lupan in its entirety:

Interviewer: How would you describe relations between Russia and Moldova since Moldova signed the Association Agreement with the European Union in 2014? Can you elaborate on any role Russia may have in Moldova’s domestic politics with regards to the breakaway region of Transnistria?

Vladimir: We have attempted several times throughout our history to approach the European Union, with the idea of becoming a member of the European Union. Most of the time it resulted in some form of intervention either by Russian or Moldovan political forces related to Russia or statements made by Russia itself, because this is how it works in Moldova. It also works with economic embargos. Russians have repeatedly introduced embargos which essentially blocked Moldovan goods from being exported to Russia which was one of its traditional markets. This happened in 1999 when we had a multiparty agreement signed and in 2000 when we had a constitutional change. This was when the Communist Party had to re-register its name to the “Party of Communists of the Republic of Moldova” and they entered the election on the wave of economic crisis and nostalgia for the Soviet Union, focusing on the relation with Russia, not with the European Union. So, for them
that was the message they sent throughout the election: we will enter a Russian union as well. As you can see, if you look at the map there is a problem because in between Russia and Moldova there is Ukraine which divides us. At that time relations were better between the two, which is a different issue, however in 2003 due to internal and external pressures the Party of Communists failed to sign a memorandum which would essentially put Moldova in Russia’s pocket. Part of this is related to the way in which Russia has used the Transnistria conflict to maintain influence in Moldova. It was the Kozak Memorandum. Putin’s chief of staff was in charge of that agreement, Dmitry Kozak. This agreement basically provided Russia with veto powers through the separatists, as the separatists alone had veto power on foreign policy and the Constitutional Court, when no one else in parament would. It was well known, in the 2000s we were moving closer to the EU. In 1998, there was even a partnership agreement with the EU and we began negotiating the partnership agreement in 1994 and it was agreed to in 1998. In 1999-2000 there was an agreement to upgrade the partnership. Moldova only became independent in 1991 and started negotiating with the EU in 1994 so it was only three years. Moldova has a history of moving towards the EU, practically from its independence but Russia showed its true face with the Kozak Memorandum. What was the purpose of this exclusive veto power for the separatists? It is to give them autonomy and Russia has influence over this faction. It’s is purely an attempt to grant them leverage over
Moldova. They would have the power in the decision process, we called this the Transnistria-ization of Moldova. Later, you also saw the Transnistria-ization of Ukraine and the developments were essentially the same. This process involves federalization which sounds good but the plan was written by Russia in such a manner to give a small actor veto power over the larger actor be it Moldova or Ukraine while Russia maintains influence over that small minority. You can even see these same tactics being applied in the United States, it’s a different matter but during the 2016 elections there were numerous succession groups in the United States that were supported by Russia. In this way Moldova is a testing ground. However, in 2013, in Moldova you saw a backlash both internally and externally which caused the Party of Communists to reject the Kozak Memorandum and Russia responded harshly with the embargo of wines and manipulation of energy, in the form of gas, prices. It was a form of punishment. You could see Germany paying less for gas than Moldova even though it is farther from Russia. The EU does not act with a single voice so it’s much easier to attempt to divide and conquer the member states. It’s worth remembering that Vladimir Putin was the head of the KGB an organization that had worked on dividing and conquering Europe for years.
Interviewer: You’ve called Moldova a testing ground for Russian political interference on Twitter and in response to the Russian disinformation campaigns in July, 2017, the Moldovan Parliament finally adopted an Anti-Propaganda Law. Can you explain what prompted the law, how it was justified and received domestically and if you believe it’s proving effective?

Vladimir: When I say Moldova is a “testing ground” you have to understand that I’m referring to the use of proxies, and by proxy, I mean a military that will do the dirty work without wearing your insignia. This concept is equally applicable in all Russia’s efforts and not necessarily only military. Try to be more flexible in your thinking. Whatever means Russia can find in a country to use it against that country, if it is a political party or a paramilitary, if it’s a struggling population longing for some specific relation or benefits from Russia then they will become a paramilitary, if there is a hacker who is interested in making the government pay a price, for example Edward Snowden and the U.S., then they will use that against the country. They will use Wikileaks to release documents or when possible, they will use their own “patriotic” hackers to release any data when possible. With the anti-propaganda law, this law is theoretically welcome in Moldova because it is blocking Russian propaganda, however it is all about implementation and when it comes to implementation, Mr. Plahotniuc appears in all the news. The news still has Russian content, or its about Mr. Plahotniuc, [the former chairman of the
Democratic Party of Moldova and a media magnate] so he essentially transforms the Russian messaging into political messaging about himself. This is not even a pre-electoral message, this is essential a propagandistic message, the type that Russia had been using but he has transformed to serve himself. The use is duel actually. You block the Russian propaganda, show the West “look I’m protecting against Russia” and then he adapts their tactics and uses it against our own population and against internal enemies. If you look at opinion polling, Mr. Plahotniuc is not very popular right now, what is important for him, is popularity, he needs to be elected somehow.

Interviewer: Pro-Russian media in Moldova have been spreading news of the imminent restitution of historical land and property held by Ukrainian citizens to Poland and likewise Moldovans having to return land and property to Romania. According to these fake reports, the Association Agreements that both Ukraine and Moldova signed with the European Union in 2014 calls for such restitution. The Association Agreement calls for nothing of this sort. What effects have such online “fake news” sources had on Moldova and how can “fake news” propagated online be neutralized?

Vladimir: It’s funny you mention this. These stories of Moldova having to give territory back to Romania. Here in New York, I was sitting with my Russian barber and he asked me about this very issue. He asked
me why Moldovans would accept giving up territory in order to join the European Union. I asked him where he had heard this and he pointed to his television. It was on Russia-1 [a state-sponsored, Russian language channel carried internationally]. I told him it wasn’t the case which he had trouble believing. This is occurring all the time and because there are few channels here in Russian many Russians who live abroad see these types of reports. They have an effect. There is disinformation but you should look up the concept of Whataboutism by the journalist Michael Bernard, its similar to the tu quoque logical fallacy. It is a technique the Soviets used where if someone says something critical, you change the topic to something distracting and more preferable. Americans would object to a specific Soviet human rights abuse and the Soviets would counter with something like “What about racism in America?” Obviously, both aren’t good but the objective of the person using Whataboutism was to change the subject. How can “fake news” propagated online be neutralized? Well, as we saw, this is difficult. There can be laws but as in Moldova you have to see the details of those laws.

Interviewer: Russia’s foreign military intelligence agency, the Main Intelligence Directorate (GRU) and the Federal Security Services (FSB) are believed to have played a part in Russia’s interference in the 2016 US presidential election through online groups respectively known as “Fancy Bear” and “Cozy Bear” by penetrating the Democratic National
Committee (DNC) in 2015 and releasing stolen and compromising information at a time when it would have the greatest political impact. Have you seen any comparable efforts in past Moldovan elections or do you suspect they could take place in next year’s parliamentary elections?

Vladimir: In Moldova, the tactics used by Russia are more brazen. They can use tactics they wouldn’t dare to use in the United States. Rather than covertly attempting to manipulate an election, they can afford to be overt in their support of a party or candidates. This is combined with disinformation against candidates who stand up to Russia or promote deeper integration with the European Union. In this was the situation is different between Moldova and the United States.

Interviewer: Russia has a long record of targeting outspoken critics in an attempt to delegitimize them in the public eye. Considering your position and outspoken criticism of Russian propaganda campaigns, have you had any experiences with cyber intrusion or attempts to compromise your character that you would be willing to share?

Vladimir: This occurred when I was serving as the Ambassador & Permanent Representative of Moldova to the United Nations over the Russian involvement in Syria. There were Russian media reports claiming I had proposed rescinding Russia’s veto authority on the United Nations Security Council. This is impossible. There is absolutely nothing in the
UN Charter about removing a Security Council member’s right to a veto. There is no mechanism for that, so it would be impossible. This was about building pressure diplomatically. Similar circumstances happened to others at the UN over Russian involvement in eastern Ukraine. As you know, Moldova is not on the Security Council and even if it was, there is no way to take away a veto from a Security Council member. It fits a pattern though, they take elements of truth, in this case, another diplomat had proposed a resolution in which veto authority would be challenged on a one-time issue for countries that prevented serious inquires on war crimes, crimes against humanity or genocide and shape it to their purposes.

Interviewer: What are the long-term objectives of Russia’s cyber aggression and propaganda campaigns?

Vladimir: The purpose of Russian ops is not only to deceive the West but also to destroy the values of the West. They target our collective values. They want to destroy the rule of law in these countries. They want to undermine the EU and NATO. They do this by bashing relations between countries with things like gas price manipulation and they do it within countries by bashing certain political parties. It’s about freedom to act. It’s about realpolitik, when certain national security issues are present, Russia understands realpolitik well and they use the resources available. Essentially, Russia sees the United States as a country that can prohibit
them, for external and internal reasons, from expanding. Therefore, any attempt by an administration to try to stop Russian actions will actually face some sort of response. In order to solve a problem, you need to have a willing partner, that’s the bilateral part of negotiations, you need to agree on a certain set of actions, up to now I have not seen Russia willing to stop. What we’ve see is Russia trying to restore its status as a superpower, which they are incapable of. They are a regional power but not a superpower, they cannot do more than that.