United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Russian Weaponized Social Media: How the U.S. Government Should Organize to Defend Against Future Operations Version 29 Apr 2019

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Jonathan B. PayCheck, Civ, DIA

AY 2018-19

Mentor and Oral Defense Committee Member: Dr. Richard Dinardo, Ph.D
Approved: R.J. DiNardo
Date: 1 May 2019

Oral Defense Committee Member: Dr. Jorge Benitez
Approved: Jorge Benitez
Date: 1 May 2019

Executive Summary

Title: Russian Weaponized Social Media: How the U.S. Government Should Organize to Defend Against Future Operations

Author: Jonathan PayCheck, United States Defense Intelligence Agency

Thesis: Using NATOs lessons to help develop better coordination and organization for a US interagency whole of government approach to deal with disinformation campaigns over social media in order to minimize exploitation of US vulnerabilities is the approach the US government should be taking.

Discussion: Social media is a weapon that the U.S. hasn't learned to defend itself against, yet. Russia is using social media extensively in modern-day gray zone conflicts capitalizing on the ability to use Cold War era disciplines in new technology driven battle zones. In particular disinformation is used against United States (US) and NATO targets today on social media war-fronts to impact political decisions, influence populations, and destabilize governments. Disinformation is being used as a soft power tool for political and strategic gains. Russia is a crucial offender as seen in the disinformation campaigns waged during the 2016 US presidential elections and operations in 2007 Estonia. Russian disinformation campaigns are a vital piece in their political warfare doctrine called active measures, which falls within hybrid warfare tactics. Using our NATO partners lessons to help develop a US interagency whole of government approach to deal with disinformation campaigns over social media in order to minimize exploitation of US vulnerabilities is the approach the US government should be taking. This paper will specifically discuss the historical background of Russian disinformation campaigns, give insight into what a Russian disinformation campaign looks like, discuss how the Russians have conducted a disinformation campaigns in Estonia, and conclude with a recommendation for what a whole of government approach might look like to combat social media delivered disinformation. The primary focus will be on disinformation tactics used in social media and the need for more coordination between agencies within the US government, to include the Department of Defense (DoD) and the Department of State in order to implement a clear approach to future Russian disinformation campaigns. US response to foreign disinformation campaigns have been limited and require more manpower and quicker response times. The current level of response effort has improved in the last few years but these efforts still fall short leading to slow reaction times to attacks that do little to stop or even minimize damage. Exposing Russian disinformation campaigns quickly is vital to winning a war of ideas with counter information operations based in truth.

Conclusion: An organizational structure similar, but not the same, to what was implemented within the US intelligence community creating the ODNI and cross communication like the EU StratCom Office is necessary for success in combating disinformation. The multitude of agencies and DoD units conducting messaging operations against US adversaries across the globe requires coordination. Clear avenues for that coordination will allow for better messaging, increase US credibility, and the ability to quickly counter disinformation campaigns like Russia's.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE, THE UNITED STATES DEFENSE INTELLIGENCE AGENCY, OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

Page

EXECUTIVE SUMMARY II

DISCLAIMER III

TABLE OF CONTENTS IV

INTRODUCTION 1
- Social Media is a Weapon 1
- Baselining Hybrid Warfare Terminology 3

KNOWING RUSSIA 4
- Understanding the Problem 4
- Knowing Russia's Disinformation History 6

DISINFORMATION AND SOCIAL MEDIA 10
- What the Disinformation Campaign Looks Like 10
- Disinformation Over Social Media 11

ORGANIZING FOR THE FUTURE FIGHT 14
- Structure is Complicated and Coordination is Needed 15
- The Concept for Cross Coordination 19
- The Global Engagement Center 22

CONCLUSIONS 26

ENDNOTES 27

BIBLIOGRAPHY 29

Introduction

"I believe that President (Vladimir) Putin has clearly come to the conclusion that there's little price to pay here and that therefore, 'I can continue this activity…in all fairness you can't say nothing has been done but clearly what we have done hasn't been enough."

Director National Security Agency Admiral Mike Rogers,
Armed Services Committee hearing 27 February 2018

Social Media is a Weapon

Social media is a weapon that the U.S. hasn't learned to defend itself against, yet. Russia is using social media extensively in modern-day gray zone conflicts capitalizing on the ability to use Cold War era disciplines in new technology driven battle zones. In particular disinformation is used against the United States (US) and NATO targets today through social media to impact political decisions, influence populations, and destabilize governments. Disinformation is being used as a soft power tool for political and strategic gains. Russia is a crucial offender as seen in the disinformation campaigns waged during the 2016 US presidential elections and in earlier operations such as Estonia in 2007. Russian disinformation campaigns are a vital piece in their political warfare doctrine called active measures, which falls within hybrid warfare tactics. In order to minimize the exploitation of US vulnerabilities, the US government should be utilizing lessons from NATO and needs coordinated organizational approach to help develop a US interagency whole-of-government approach to countering disinformation campaigns, particularly those within social media.

This paper will specifically discuss the historical background of Russian disinformation campaigns, give insight into what a Russian disinformation campaign looks like, discuss how the Russians have conducted a disinformation campaigns in Estonia, and conclude with a recommendation for what a whole of government approach might look like to combat social media delivered disinformation. The primary focus will be on disinformation tactics used in social media and the need for more coordination between agencies within the US government, to

include the Department of Defense (DoD) and the Department of State in order to implement a clear approach to future Russian disinformation campaigns. US response to foreign disinformation campaigns have been limited and require more manpower and quicker response times. In the last few years the level of US response to disinformation has improved but these efforts have slow reactions times that do little to stop, or even minimize, damage. Exposing Russian disinformation campaigns quickly is vital to winning a war of ideas with counter information operations based in truth.

If there is any doubt that Russia is out front of the United States in the use of "social media as a weapon" then those doubts should be washed away after seeing Russia's attacks on Estonia and the US. "The use of cyber and social media has significantly increased the impact and the capabilities that obviously this has been done for years and years, even decades," said Director of National Intelligence Dan Coats. "But the ability they have to use the interconnectedness [of the Internet] and all that provides ... they literally upped their game to the point where it's having a significant impact."[1] Former Director of the Central Intelligence Agency, John Brennan, said "It's not just the Russians that pose a challenge in that context as far as our future elections and election processes," he said. "We're vulnerable to other attempts—whether they be domestic or foreign… There really needs to be a better sense of exactly how the government is going to fill its responsibility to keep its citizens safe and secure and carry out the rule of law in this environment where, in some respects, it's like the Wild Wild West."[2] The US needs to look to those in the world who are fighting back, like our allies in NATO.

Baselining Hybrid Warfare Terminology

As previously mentioned, Russian disinformation campaigns fall within the realm of hybrid warfare. It is difficult to explain what HW is because there is no one clear definition

established or accepted within the US Department of Defense (DoD) or other combat support agencies. For this discussion, the term hybrid warfare will refer to State HW, as explained by Dr. Patrick J. Cullen at the Norwegian Institute of International Affairs, which involves “the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.”[3] Additionally “Hybrid warfare is designed to exploit national vulnerabilities across the political, military, economic, social, informational and infrastructure (PMESII) spectrum."[4] Part of the political and social aspect to the "divide and conquer" tactics of disinformation through social media platforms is a major underlying element to State HW. Disinformation campaigns are just below the threshold of military conflict, “gray zone,” targeting the seams of culture and society to destabilize a nation while allowing an avenue for plausible deniability. Russia is fighting in the gray zone and using social media to further its goals, sparking unrest and amplifying issues in other countries. Russian hybrid warfare follows the “Gerasimov doctrine,” named after the Russian chief of general staff who developed the doctrine, which states, “The lines between war and peace are blurred.”[5] Between these lines is where Russia uses HW and social media disinformation.

A simple explanation of hybrid warfare by Douglas Cantwell sums it up in fewer words, “The best way to boil a frog; the adage goes, is to turn the heat up slowly enough that the frog doesn’t realize it is being cooked. If the perpetrators hacked the stove’s software, denied their culpability, and bombarded bystanders with fake news before annexing the kitchen, one might have a useful analogy for hybrid warfare.”[6] The fake news bombardment, in this example, are the disinformation over social media pieces that have been influencing populations in order to destabilize nations.

Knowing Russia

"I think the United States, we have an organization to effectively operate, what we need to do is policy and things that flow from that, a whole-of government approach, that's not what we have in the way that we need it today. … We have an adversary here who's using it to very good benefit."

Army Gen. Curtis Scaparrotti, U.S. European Command,
Senate Armed Forces Committee Testimony 2017[7]

Understanding the Problem

Figure 1 High-resolution map showing the connections between Facebook's 600 million users in 2010. (Paul Butler/Facebook). Facebook users are able to be influenced within an instant by foreign actors. A perfect platform for Russian disinformation campaigns.

Why does Russia use disinformation on social media? Russia uses disinformation in all forms of media but the internet allows them to spread that fake information even faster and farther than ever before. Disinformation as Russia is using it on social media is meant to destabilize, create divisions and create chaos by spreading rumors quickly and amplifying current day issues to stir emotions and controversy. Facebook believes Russia has reached over 126 million users on its platform with its disinformation campaigns, while Twitter has found 2,752 Russian-linked accounts and over 36,000 bots spreading tweets related to Russian campaigns.[8, 9] The disinformation fight is taking place in a civilian space where many US government agencies have no real office or true understanding which makes it difficult for

government departments like the DoD to function or fight. Making matters worse, the majority of policy makers are generationally out of touch with understanding the true threat of social media disinformation campaigns. There was no military or government office protecting social media forums from disinformation or foreign attacks in recent years past. CYBERCOM and DHS do not monitor these areas for disinformation but arguably DHS would be better suited to assist DoD in this fight when it touches the continental United States (CONUS). Outside US borders disinformation campaigns are a piece of the more massive HW campaign that DoD and the Department of State (DoS) have to learn to fight defensively now and arguably offensively in the future when its service-members and employees are abroad. Developing clear procedures for who will handle and coordinate efforts in this fight and how it will be fought are needed now.

The inability for many within the DoD to clearly define why social media matters and what hybrid warfare looks like are signals that they might be behind the curve of their competitors in Russia. Russian cyber and intelligence officers have been working on foreign language perfection for as long as the US has been complaining that something needs to be done about the slack of language expertise in US offices. The US has been struggling with a language gap that has increased over the past 15 years.[10] It is reported that the Russian government employed over 600 people who implemented the social media attacks in the Crimean war in 2014 spending over $19 million to instill hate and fear that would sway public and international opinions.[11] Great Britain has an ongoing investigation to understand if Russian actors used Twitter to influence the Brexit vote in 2016 as many of the Twitter accounts were the same used to spread disinformation during the 2016 US presidential campaign.[12] In 2007, Russian disinformation campaigns not only attacked Estonia's entire government, banking system, and social media platforms, but they were also used to incite riots, a possible backlash to them for

joining NATO. Some see the attack on Estonia was a decisive victory for Russia because the cyber-attacks were not stopped until the Estonian government was forced to temporarily cut its international connections to the Internet.[13]

Knowing Russia's Disinformation History

Russia has a long history of using disinformation, creating an office for disinformation in 1923[14] and has used it tactically ever since. Dezinformatsiya first received institutional status in 1959 when the Soviet KGB established a special unit in its First Chief Directorate known as the "Department for Active Measures" who specialized in black propaganda and disinformation.[15] Disinformation is a part of Soviet political warfare, which the Russians refer to as "active measures," used to influence the course of world events customized to fit the target nation and which now includes platforms such as social media. Active measures have continued in the post-Soviet era in Russia as they attempt to destabilize relations with NATO countries and US interests. .[16, 17, 18] In response to Active Measures the Russian Information Group (RIG), designed to support "a credible counter-Russian voice" in Eastern Europe was established. The RIG began as a result of the Fostering Unity Against Russian Aggression Act of 2017 (H.R.3025). According to General Curtis Scaparrotti commander of the U.S. European Command, the RIG "has to be reinforced, it has to be financed, they have to have the authorities that they need to lead that forward."[19]

The use of disinformation, the deliberate spread of false information in order to deceive, within information warfare is not a new tactic by Russian political leaders, intelligence agencies or military.[20] The very term disinformation in its English form did not arrive in English dictionaries until the late 1980s and was taken from the Russian word dezinformatsiya which derived from KGB black propaganda operations.[21] Black propaganda is false information that

claims to be from one side of the conflict but is actually from the opposing side. “It is typically used to vilify, embarrass, or misrepresent the enemy.”[22] There is also gray propaganda which has no source, and white propaganda which is sourced correctly. All forms of propaganda could be used in a disinformation campaign over social media. Many social media campaigns take both sides of an argument or heated topic using all types of propaganda in order to spread lies, creating confusion and furthering Russian goals motivated by their national interests.

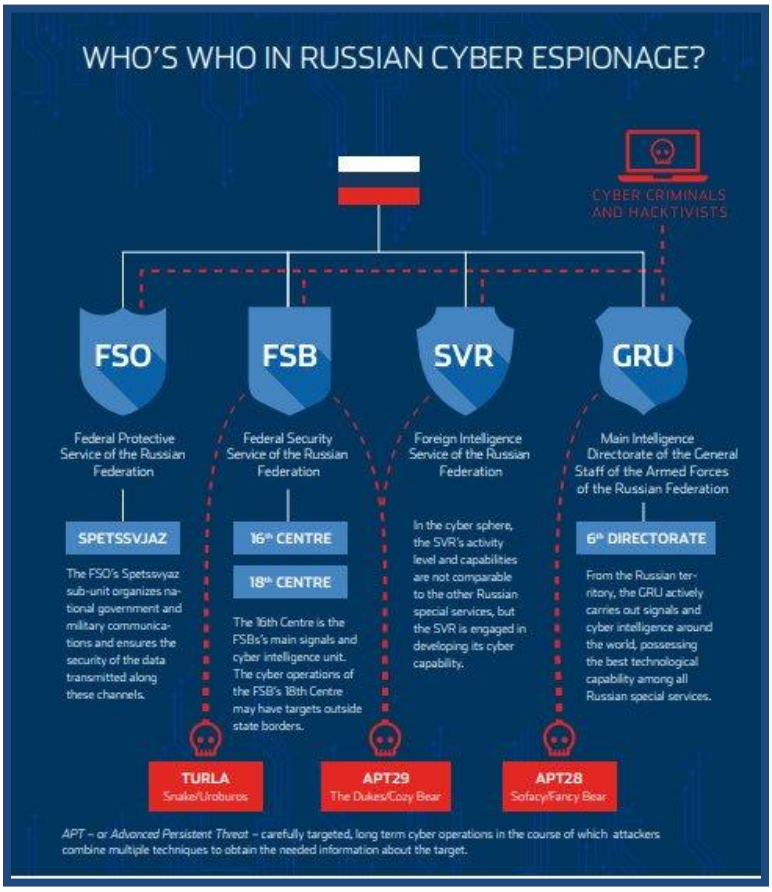

Figure 2 After the dissolution of the Soviet Union, KGB signals intelligence functions were divided between three Russian special services: the federal security service FSB, the foreign intelligence service SVR and the federal defense service FSO. In addition, GRU[23]

The Russian chain of operations for disinformation campaigns starts with Russian President Vladimir Putin, Russian military leaders, GRU leadership and others. The campaign is distributed to attributed and unattributed sources like the news state owned channel Russia

Today and radio station Sputnik. Unattributable sources like the Internet Research Agency, a Russian private owned but government supported agency, that supply's Russian trolls to distribute disinformation to amplification channels like Facebook and Twitter. The chain ends with the consumers of the disinformation campaign who also help amplify it by continuing to believe and spread the lies originations in Russia.[24]

Some Russian disinformation strategies can take years to be implemented in accordance with Russian doctrine.[25] Russia has cyber intelligence programs that fall under advanced persistent threats (APTs). These are long-term multi-disciplined intelligence projects with specific targeting that can remain in place for years. The goal is to further Russian national interests via the APTs. Shown in figure 2, APT29/Cozy Bear is one such program that employed social media disinformation campaigns as part of the overall project. Defending against multi-disciplined APTs like this are a reality that the US and its NATO allies are dealing with today. NATO countries like France and Estonia have lessons the US can learn from.

Historically disinformation or propaganda has been used by Russia to mold and develop their nation and to weaken their enemies. In an attempt to damage the United States in 1984 the Russian KGB posed as Klu Klux Klan members in a Los Angeles rally during the Summer Olympics and published racist material to take advantage of an unstable environment in order to destabilize national opinions of the United States.[26] Today, Russian bad actors use Facebook ads both to promote the social movement Black Lives Matter and simultaneously label the organization as a dangerous threat.[27] The GRU's (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, formerly the Main Intelligence Directorate) tactics have not changed much over the years, but the way to implement these tactics has been hugely successful with the assistance of digital pathways like social media. The Russian information

warfare doctrine has two areas in which they concentrate their capabilities and tactics, information-technical and information-psychological. Disinformation campaigns fall into the information-psychological area but are implemented via the cyber avenue of information-technical capabilities.

Propaganda and disinformation are similar and could both be perceived as damaging to the US' reputation if they were to use them. The US should stay away from the business of spreading lies. Instead, the US should fight disinformation by spreading the truth. At the end of the Cold War, the US was working with propaganda but took a turn to use less of it due to public backlash as it is perceived as the government being dishonest. Russia did not stop using propaganda to their advantage and have a thriving disinformation program dating back decades that now falls under the GRU. The psychological or influence programs within our government now are minimal in comparison to nations like Russia with peer level capabilities. The Russians have continued to use disinformation against their citizens and the rest of the world, now with the internet allowing them to spread information much faster. Russia also saw the possibilities of long-term effectiveness using a cyber strategy that would include propaganda or disinformation in an information warfare front. Up until after 2017, the US has been extremely slow in adopting the concept of information warfare at the level Russia has. The Russians have gained a huge base of real-world experience to work from. Defending against their experienced influence attacks will be extremely challenging for domestic offices in the United States and military units abroad.

There have been many active measures campaigns but some of the most recent being the operations conducted against Estonia in 2007 and the 2016 US Presidential elections.[28] These disinformation campaigns over social media are meant to assist other operational efforts by Russia to end in a desired outcome favorable to Russian policies. "Many European governments

are taking proactive steps to counter Russian propaganda and disinformation efforts. NATO has prioritized efforts to counter "hybrid threats" by developing a strategy that includes strengthened coordination with the European Union, as well as training and exercises through its new Intelligence Division. The Strategic Communications Center of Excellence in Riga, Latvia and the Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia also contribute to these efforts. In addition, several NATO allies and European Union members signed a Memorandum of Understanding to establish a European Center of Excellence for Countering Hybrid Threats in April 2017."[29]

According to Dorothy Denning, for decades "Russian operators have stolen terabytes of data, taken control of millions of computers and raked in billions of dollars. They have shut down electricity in Ukraine and meddled in elections in the U.S. and elsewhere. They have engaged in disinformation and disclosed pilfered information such as the emails stolen from Hillary Clinton's campaign chairman, John Podesta, following successful spear-phishing attacks."[30] The 2007 French elections saw protests by the "Yellow Vests" movement which Russia sought to amplify street protests, create division amongst the people and government, and create general chaos about the movement though social media disinformation posts.[31] Russia seeks out divisive issues in order to exploit them for immediate or long-term gain. The Russian government is leaning forward and is successfully setting the stage for follow on events of their political and military choosing.

Disinformation and Social Media

"Russia seeks veto authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, to shatter the North Atlantic Treaty Organization and change European and Middle East security and economic structures to its favor. The use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough,"

Secretary of Defense James Mattis, 2018 National Defense Strategy

What a Social Media Disinformation Campaign Looks Like

A high-level view of a disinformation campaign in its most basic form is simple to understand but laborious to undertaking and difficult in practice. There are very few base steps in the process, but there can be more branches and sequels to an operation. The first item in a campaign is to identify what the campaign will target, a divisive issue or topic that can have a believable simple narrative applied that is easily understood, highly emotional, and has some credibility. The target must be something that will end in the support of the attacker's goal. In Russia's case it might be eroding trust between the US and a NATO partner like France or Estonia. Second, research must be done on the target to determine where the weak points are. This can take time but, in most cases, it can be done in a matter of hours over the Internet. Third, the antagonist must choose a weak point that is divisive or sensitive in nature; then mount an attack by choosing a side (or both) in which one can achieve the desired result. The fourth item would be to continue to feed a successful campaign by continuing to spread disinformation or starting the process over again until the required result is reached.

Disinformation Over Social Media

Disinformation can be spread through many different avenues such as print news media, tv/radio/internet news media, and now social media. Social media allows for an agent or spy to skip the step of having to find a sympathetic journalist, trusted contact, or other agents of influence. Social media is possibly even more effective than state-run media or television stations like Russia Today, since an agent or "troll" can reach a broader audience and spread a story much quicker through sharing and likes.

For a disinformation plan to have a better chance to be successful, it may need to be followed up with by other capabilities like cyber operations, economic pressure, support for local opposition groups, criminal activity, or more disinformation. All of this could involve the

deployment of covert operators (spies), regular troops, irregular troops (including unmarked troops), contractors (trolls), or other cyber operators. In the past disinformation was created and implemented by government intelligence organizations with an accompanying concept of an operation that supports the states strategy. However, today we can see that Russian state-owned or contracted private industry are being used to implement and create plans that are successful. This change is due in part to the advent of social media networks and the internet as a whole and the plausible deniability that outsourcing brings.

Today the best avenue to mount an attack on Western minds in the US is via social media. As of August 2018, 68% of Americans get some of their news from social media forums, see figure 3.[32] People receive their news through social media and then pass the disinformation on at a pace hardly imagined just ten years ago. The typical spy tradecraft needed by an agent working in disinformation distribution are no longer required with access to millions over the internet at the spy's fingertips. Recruiting someone to spread disinformation within a news organization or other means are not needed now with a social media post taking its place and with the possibility of distributing to a larger populace.

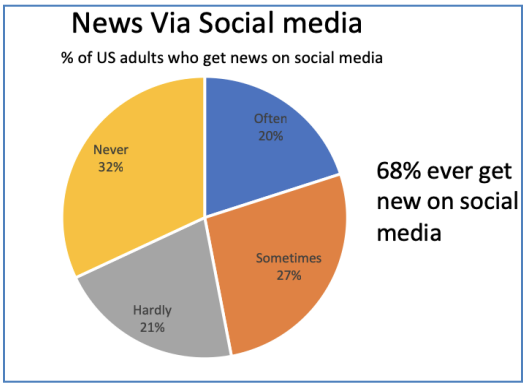

Figure 3. Pew Research Center study shows many Americans get their news from social media and this number has grown every year since 2013 even if the trust that the news is accurate has declined.[33] [34]

Cyber operations and social media have changed the way disinformation campaigns are being conducted and are more effective. The United States and Estonia have both seen firsthand how easily a foreign government's disinformation campaigns could create confusion. In Estonia in 2007, Russia stoked the flames within Russian-minorities to start riots and followed with a cyber-attack to shut down banking and government systems. In 2016, Russia conducted influence operations to sway public opinions during the Presidential elections. Russian operations have played on race and ethnic issues and fears of the citizens while simultaneously using real-world controversies and issues being discussed by the populace. By obscuring the facts, inflaming real issues and imbedding lies on social media through memes, fake news stories and postings from intelligence operatives acting as local citizens or organizations, the Russians created confusion and divisiveness amongst the population. Operations in Estonia were successful in brining their nation to a halt, the US cannot allow a similar occurrence.

A significant advantage in social media disinformation campaigns compared to historical disinformation campaigns are the speed and expansive reach that just a few postings on social media has. The shortfall is in the numbers needed to make the campaign effective. The GRU alone does not have the personnel to take on a big project like this in order to sway a population. Like many countries Russia has turned to specialized contract assistance, Russian pro-Putin financiers created a private company called the Internet Research Agency to employ "trolls," people to make posts across multiple social media accounts using different personalities in order to stir up controversy.[35]

The term "troll" is a little misleading in the sense that Russian trolls are not social media users trying to get a simple rise out of people. Russian trolls are paid to stir up controversy and inflame issues within a target country in order to destabilize it. These trolls are given a directive

and a target by leadership within the Russian government. They broadcast specific messages and themes designed to further Russian strategic goals. They use fake accounts created to specifically do the job described. The average "troll" does not operate like this; Russian trolls are professionals.[36]

With thousands of trolls to do the work and implement the disinformation campaign, adversaries are preyed upon easily. The initial concept of the operations for a social media campaign are more sophisticated than the actual propaganda messaging; it is not hard to cause strife over race, politics, jobs or religion. The tactics used in Estonia in 2007 exploited small, domestic disagreements about moving the statue of a Russian war hero. Foreign agitators helped turn the protests into riots with one person being killed. Social media trolls were used to stir up the controversy and create strife in Estonia until it boiled over into the real world. We may never really know how successful or unsuccessful campaigns are but the campaign in Estonia did cause chaos and took an entire country's government off line for three weeks. The disinformation and cyber-attack on Estonia could easily be considered a success for the Russians.

Russia has a recipe for its campaigns and it does not change much as it switches targets. The same tactics Russia used in its disinformation campaign to influence the Estonian citizens will likely to be used against the United States in the next "below the threshold of war" conflict. The Baltic nations have been dealing with Russian aggression of this sort for years now, their model should be considered by the US as a frame work in its efforts to take a more focused approach against this modern spin on an old threat. Civilian volunteers, knowing how to rapidly get out in front of disinformation with the truth, educating government officials and the populace has helped countries like Latvia push back against Russian disinformation.

Organizing for the Future Fight

"The security environment is also affected by rapid technological advancements and the changing character of war. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology-the very technologies that ensure we will be able to fight and win the wars of the future. "

Secretary of Defense James Mattis, 2018 National Defense Strategy[37]

Structure is Complicated and Coordination is Needed

When a disinformation campaign is discovered, the best response is a counter information campaign of truth and transparency. This defensive response could include exposing the attacker in order to discredit future disinformation campaigns from the source. Unfortunately, like opening Pandora's box, once disinformation has spread it is nearly impossible to neutralize the effects of that information on a population. The idea will remain regardless of what counter campaigns are implemented to spread the truth or what damage control measures are attempted. It is critical that campaigns be exposed early (preferably within the first 24 hours) which is much more difficult now in a digital media environment.

Legally, once the focus of an attack has found the attacker's location, whether within or outside the United States, will determine the responding organization for a counter campaign, such as DoD or the DHS. For attacks outside the United States the DoD would be able to work with the Department of State's Global Engagement Center (GEC) and our NATO partners.[38] In 2016 the US State Department created the Global Engagement Center pursuant to Executive Order 13721 and brought into law in 2017 in the National Defense Authorization Act (NDAA) by Congress. The GEC was initially created to counter terrorist messaging campaigns but has since added state propaganda and disinformation from foreign adversaries to its work load. For attacks that originate from within US borders a similar counter campaign will need to occur but it must be handled by domestic agencies like the FBI and DHS. For the sake of simplicity, this

paper focuses more on developing an organizational solution to better counter targets outside of US borders using a whole-of-government approach.

The US government has difficulty in discussing the issue of disinformation campaigns over social media as many are not educated about disinformation over social media. Yet, those affected by it and those who should be responding to it need to know more about it. There is a sense that US counter-disinformation is seen as propaganda instead of soft power that can be used to combat peer competitors' disinformation campaigns. Delicate discussions should be had to reassure policy makers that combatting disinformation with the truth is more effective than attempting to combat it with more lies. Educating the public and government on how these campaigns happen and what tools are being used to fight it, as well as what is being used against us may help with transparency. Educating government officials and the US population on being good consumers of information over the internet is vital to the success of combating disinformation. The public and government must both approve of the tools necessary to combat these attacks against our nation, otherwise it will appear the US government is hiding something.

In Europe the attitude toward fighting disinformation is much different because they are living next to the Russian threat. Daniel Kimmage, GEC Director stated that Europe is working in the right direction "The European Commission Code of Conduct is an excellent step in the right direction, the establishment of centers of excellence in Riga, Tallinn and Helsinki to study and address aspects of this challenge is also significant. Governments across Europe are taking this fight seriously. The Swedish civil contingencies agency spent the year leading up to Sweden's recent election, canvasing the world to find the best approaching to addressing foreign influence in elections...the Czech government invested in its Center for Terrorism and Hybrid Threats to coordinate a government wide effort to address disinformation and

propaganda…media literacy is part of the high school curriculum in Italy."[39] The initiatives are growing rapidly in Europe to combat disinformation. Estonia was a highwater mark but the attack on Ukraine was the next unexpected step by Russia with even larger consequences. The EU and Baltic states have established a good foundation for organizing the effort, educating the public, and cross government coordination. The Baltic states don't have this issue solved but they are further along than the US at present.

When a campaign is launched against the US one approach is to ignore the disinformation giving it less credibility. In some instances, this may be the best approach but for the majority of cases action is required. If left untouched it may create unrepairable damage to the government and the trust that binds allies. The campaign could be designed to lay the groundwork for an enemy to breach trust with another nation or allowing the enemy to take credit for good deeds done by the US. Russian campaigns need to be met with force quickly in order to minimize internal damage and to respond to the offender immediately. The steps to respond to an attack require a lot of human capital and training, consistent monitoring of social media similar to a news agency, and responding with truthful messaging that is coordinated across the government in order to render the disinformation ineffective.

According to GEC Deputy Coordinator Jonathan Henick, educating the population is a major key in order to defeat a disinformation campaign.[40] Publishing news stories and social media content that inform the public of the truth will expose the enemy. There are volunteer pro-government teams within the Baltic countries like Estonia and Latvia that report on Russian disinformation campaigns and work to expose disinformation with truth.[41] Government created pamphlets on disinformation or the United Nations handbook "Journalism, Fake News, and Disinformation" are being used to inform people on how to be good consumers of information.[42]

Similar information education campaigns could be helpful in the US, the caution is that an education campaign may be viewed as biased and government propaganda if executed with a poor plan. Working with private industry or US news journalist agencies to promote education may be a more effective solution.

Additionally, the EU has established a rapid response action plan system that through the East StratCom Task Force of the European External Action Service will focus on improved detection of disinformation, coordinate a response to it and raising citizens' awareness of the issue.[43] The task force is supplemented by journalists, government officials, NGO's and Think Tanks in over 30 countries all working to root out disinformation. The East Stratcom Team is intended to develop dedicated communication material on priority issues, where EU strategic communication needs to be improved or the EU is subject to disinformation campaigns.[44] The EU, European Commission, is taking this seriously as seen by increasing the budget of the East StratCom task force from 1.9 million euros to 5 million in 2019.[45] The US will also need to invest more and more effectively to defend itself better from this type of information warfare through social media.

The US government doesn't need to dive into black propaganda to be effective fighting disinformation over social media but it does need a coordinated response through agencies like the Department of State, DHS, and DoD. If DoD expects to defend against disinformation campaigns from foreign threats like Russia, empowering military intelligence units with disinformation capabilities may help increase the manpower working against regional threats but it must be coordinated through a focal point office. A combination of cyber, private industry technology, and intelligence service members working together to counter disinformation over

social media and linked to the State Departments GEC and CYBERCOM would be a great step in the right direction for the US government being able to resolve this problem.

An enemy disinformation campaign can be stopped, but the target may never recover from its effects if the negative information spreads too far. Through counter information campaigns and an organization dedicated to detecting and countering or exposing disinformation the US can generate defensive measures to stop Russian campaigns. Currently there are multiple offices under multiple agencies working to defeat disinformation in one aspect or another. Some offices attack the problem covertly and some overtly. Some offices or agencies prefer to respond through cyber disciplines while others prefer to respond in kind via counter messaging. All these differences are correct given each individual situation, but they should be coordinated across government in order to be as successful as possible. A coordination center or focal point office is needed to organize the US governments agencies in order to reduce stove piping and duplicating efforts. Essentially, better coordination is key in making US efforts successful.

The Concept for Cross Coordination

Private industry and news media in some form need to be a part of this solution for coordinated efforts. Filtering communication and efforts through the DHS to US journalist and private tech corporations like Facebook and Twitter may be necessary for good optics and keeping US government efforts from appearing biased. For the US to combat disinformation campaigns it will require partnering with social media company leaders to coordinate with their policing efforts, developing a focal point office similar to the EU Task Force, calling on volunteers from the military and private sector to police social media, and coordinating across borders with our allies that may be more readily able to fight a similar counter disinformation campaign. Ahmed Younis, a former staffer within the GEC, seems to be under the same

impression that coordination is needed when he says there is a "need for a central unifying body that ensures all government agencies are presenting a unified front against this threat [Russia]".[46]

Within Congress, there has been debate over if the government is doing enough and why the US is not using the same model of organizing the effort, educating the public, and cross government coordination that the Baltic Nations are using to fight disinformation.[47] By supporting government offices like the GEC and offices within the DoD that are fighting disinformation the US government can form a more aggressive approach to countering these effects. Proper funding and manning must follow in order to support a central or focal point office that will manage and coordinate these efforts across government. It is imperative that US leaders acknowledge disinformation as a genuine threat and develop the necessary actions through social media monitoring, public education, and immediate reaction to such incidents.

A clear whole-of-government approach to combating disinformation is needed to face this issue. The US needs to creatively defend against these real threats to its government and citizens. The NDAA states the mission of the GEC as "lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[48] Unfortunately, the GEC is only one piece to the needed solution and has only recently been funded and manned well enough to handle the Russian problem. The GEC is in the position to be the focal point that the US government needs in order to coordinate efforts across government.

The GEC needs more expertise if they are going to take on a nation like Russia in this new battlefield of social media disinformation; the right people in the right positions. Countries like Estonia have been fighting Russian disinformation campaigns for years and have expertise

that analysts could benefit from. Expecting the GEC to accomplish all its tasks against terrorist organization recruitment and state-run disinformation is unreasonable at their current personnel state. The GEC will have a hard time succeeding at creating any empirical data that Congress will need to see in order to justify their existence in the future without obtaining the expertise needed. The GEC is seeing some of the similar growing pains that the EU's East StratCom Task Force went through in its infancy but with time and proper support they should be able to gain some ground in the fight with Russia.[49]

Within the public social media segment, social media outlets like Facebook and Twitter in the US have started to attempt to purge fake accounts created to distribute propaganda and disinformation. To what extent Facebook is actually working to make things better is unknown at this time. Facebook makes money off advertisers when views, likes, and shares raise the cost to those advertisers, while trolls and bots assist in that endeavor by raising the number of those likes and shares. Tracking down the bots and fake accounts is not beneficial to Facebooks business model even if it is the right thing to do ethically.

While Facebook and Twitter are blind accomplices in the spread of disinformation that is harming governments. Having a liaison officer through DHS could help clear up communication issues between government and private industry leaders at these organizations. It remains to be seen if these companies will do the right thing while sacrificing profits but an attempt needs to be made by government to extend an olive branch if they will help remove disinformation and deny foreign adversary's an avenue for their lies. Allowing government to help them in their fight would be beneficial for both parties politically.

Estonia is a good example of what a more resilient information warfare defense looks like. More than just removing the fake accounts and bots from social media platforms, the US

government needs to educate its people on disinformation and how its government is planning to respond so that trust and support is gained by its citizens. It is a civil affairs campaign of earning goodwill and spreading the good news about what the government is trying to accomplish in order to protect its people and freedoms. James Clapper, the former Director of National Intelligence "called for "educating" Americans about the use of disinformation and for a major push at "counter-messaging" by Washington."[50] Along with educating the people, educating service members for buy-in, understanding, and support is essential. DoD should have a similar mirrored approach as CONUS agencies, coordinating through CYBERCOM and the GEC when reporting and responding to disinformation.

Why the Global Engagement Center

The structure of the GEC is simple and allows for some flexibility. The organization has a staff office and then analytical cells organized by regional support. The coordination piece could add an entire team that would primarily focus on liaison officers given to the GEC from DoD, CIA, DIA and DHS to support efforts across government. Figure 4 gives a possible approach to coordination and communication efforts across government.

The GEC is focusing efforts on effects-based results and some policy at the moment, as well as, attempting its mandate for coordination. The current structure allows the GEC to divide its 80 employees into staff and geographical functional areas allowing for regional experts to focus.[51] The mandate by the 2017 National Defense Authorization Act instructs the GEC to take on "state run disinformation". The office was tasked with a much larger mission and just now seems to be getting its footing and funding. Currently the biggest issue is getting the right expertise in place and educating the public and policy makers.[52]

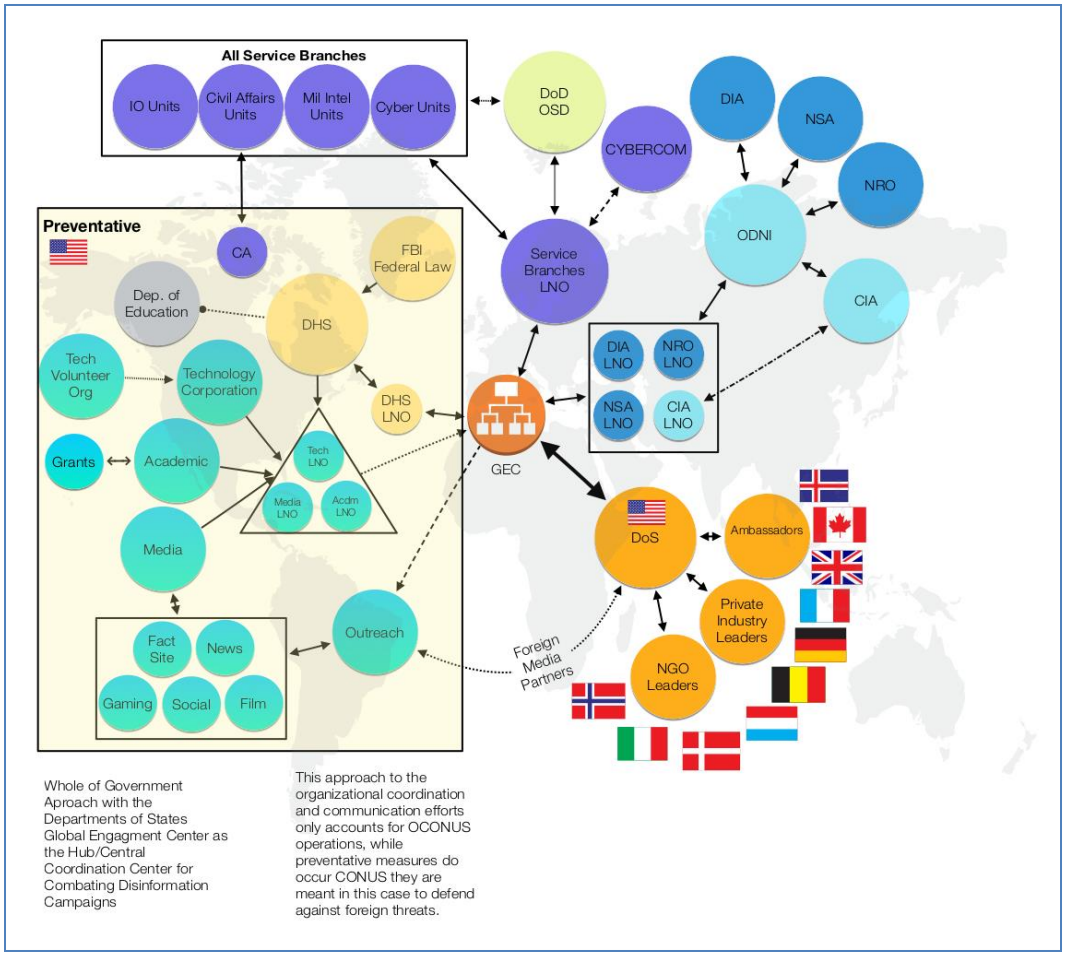

Figure 4: Depiction of the possible organizational structure for the Department of States Global Engagement Center acting as the center for coordination of countering disinformation operations. The organizations are divided partially as preventative and curative measures for defending against and combating disinformation campaigns.

The broader structure within US government needs to be stream lined with coordination across groups in order to enable better campaigns to combat disinformation. Coordination efforts will also minimize duplication of effort which can come at not only a credibility cost but also a financial cost to the US government when funds are appropriated for duplicate programs. A coordination center created to oversee operations and provide networking between offices is needed to synchronize efforts. This focal point office would act as the connective tissue that allows government organizations to work towards common goals and eliminate waste.

The whole-of-government approach by GEC is needed in order to accomplish the governments mission and is starting to happen slowly but more needs to be done. For its part, DoD needs to ensure that Information Operations (IO) units are doing more than spreading leaflets. IO and Civil Affairs teams need to be focused more on community engagement and getting good news stories out. Department of State needs to make sure the ambassadors are doing more to influence host nations to support US interests, which includes combating Russian influence operations. The good news stories need to be promoted by the government to build up US credibility. The US and even the EU do terrible jobs informing the public of the many positive services they provide and victories achieved. Informing the public on what the US is doing right and how current steps are helping improving US security, will build the good will and credibility needed in order to have the message heard when countering a disinformation campaign. If people are misinformed to not trust the government, then any efforts following will have limited success if any at all.

A future GEC would have additional personnel and an additional office that would act as the primary coordination office conducting oversight and providing transparency within the information operations community. At first the GEC should be given proper funding authority and authority to distribute funding to other agencies much like the Office of the Director of National Intelligence (ODNI). Holding funds and distributing them as needed for information operations within this community will establish legitimacy of the GEC as the center for coordination and assist with their coordinating missions. Congress would have a line of funding that is established for the GEC to distribute towards efforts within information operations programs (IOP) as needed, similar to military intelligence program (MIP) funding that ODNI distributes to the intelligence community.

Just like ODNI, the GEC would have oversight but unlike the ODNI the GEC at first would have limited or no authority to deny program execution but would coordinate efforts across government. The coordination mandate is within the GECs charter but does not seem to have been fully implemented. Coordination would include government funded efforts like Radio Free Europe. A funding line that could be used to assist those with information operations efforts would be a valuable incentive to adapt to this new structure. A large point of tension will be within the combatant commands (COCOM) to share authority and coordinate with others while having a leading civilian agency conducting oversight. In time these tensions should subside once passing information through the GEC is seen as the normative process for oversight and coordination.

An additional issue is that the bureaucratic process within the US government moves terribly slow. Conversely, information operations move rapidly over social media, giving the GEC the full authority to act or delegate to other agencies that authority would allow for more timely responses and campaign implementation. Information operations concerning disinformation can be difficult for some senior leadership and policy makers to understand. The multitude of platforms, technology and forms of social media communication can be overwhelming and frustrating. Staffing the GEC with trained experts to authorize actions, while oversight still remaining in leaderships hands, would give a leading edge that is needed in order to be competitive.

Another issue within US government is the moving away from influencing foreign governments to a state of only informing them. The State Department may not have the right people in position to honestly inffluence our foreign partners towards implementing goals that have both our nations interest. The ambassadors and embassy personnel along with special

envoys are charged with supporting US interests and not with pleasing foreign governments. A fear of losing bilateral talks with the host nation are the driving factor but this is a flawed assumption. Without local support US efforts to counter disinformation may not succeed.

Baltic countries have a deep understanding of cyber and information operations as they have been fighting Russian disinformation for years, they have an extremely permissive environment, and there is an across government approach to fighting disinformation and Russian aggression. Even with the momentum that they have, they still need support from the US government. The EU needs to be recognized for the good things they have done and are doing. The EU also didn't convey their messages for a broader audience, complex sophisticated messaging did not translate easily to simple narratives needed for the everyday person. Honest and straight forward communication of the truth is an easier way to build trust and gain commitment from the public and policy makers.

Conclusion

In conclusion, the US has established a small office, the GEC, but this will not be enough to stop Russian disinformation efforts. Learning from the EU and Baltic nations is another necessary step to improve the defense of the US. The government needs to do more to stop Russian disinformation influencing it's population and eroding it's relationships Europe. Establishing an office at the Department of State with minimal funds or personnel doesn't signal that the threat is being taken seriously but it is a step that can be built upon. Coordinating and learning from nations like Estonia who have felt the wrath of Russia's disinformation tactics and are fighting back successfully is more of what needs to happen if the US wants to defend itself better in the future.

Notes:

[1] Philip Ewing, "*Russia's Election Meddling Part of Long History of 'Active Measures'*," National Public Radio, May 23, 2017, https://www.npr.org/2017/05/23/528500501/lies-forgery-and-skulduggery-the-long-history-of-active-measures.
[2] Tanisia Morris, "*Former CIA Director Brennan: Russian Election Meddling 'Incontrovertible'*," Fordham University New, January 10, 2018, https://news.fordham.edu/colleges-and-schools/school-of-law/former-cia-director-brennan-russian-election-meddling-incontrovertible/.
[3] Erik Reichborn-Kjennerud & Patrick Cullen, "*MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare,"* (Norwegian Institute of International Affairs, Jan 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.
[4] Ibid.
[5] Hannes Grassegger and Mikael Krogerus, Translated by Edward Sutton, "Fake News and Bot Nets: How Russia Weaponized the Web," *The Guardian*, December 2, 2017, https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia.
[6] Douglas Cantwell, "Hybrid Warfare: Aggression and Coercion in the Gray Zone," *American Society of International Law: Insights* 21, no. 14, (November 29, 2017), https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone.
[7] Joe Gould, "EUCOM Commander: US needs stronger response to Russian disinformation", March 23, 2017, https://www.armytimes.com/global/europe/2017/03/23/eucom-commander-us-needs-stronger-response-to-russian-disinformation/
[8] Wikipedia Online Encyclopedia, "*Disinformation*," Last Edited October 2, 2018, https://en.wikipedia.org/wiki/Disinformation.
[9] Scott Neuman, "*Russia Using Disinformation To 'Sow Discord In West,' Britain's Prime Minister Says,"* National Public Radio, November 14, 2017, https://www.npr.org/sections/thetwo-way/2017/11/14/564013066/russia-using-disinformation-to-sow-discord-in-west-britains-prime-minister-says.
[10] Department of Homeland Security, Government Technology and Services Coalition's, Homeland Security Today, "*Shortage of Foreign Language Speakers, Linguists Still Plague State, Intel Community*," https://www.hstoday.us/industry/daily-news-analysis/shortage-of-foreign-language-speakers-linguists-still-plague-state-intel-community/.
[11] Patrick Duggan, "*Harnessing Cyber-technology's Human Potential*," Special Warfare, 28, no.4 (October-December 2015), 15, http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf.
[12] UK Parliament Interim Report, *Russian influence in political campaigns*, (United Kingdom Parliament, 2017), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm.
[13] Hannes Grassegger and Mikael Krogerus, Translated by Edward Sutton, "Fake News and Bot Nets: How Russia Weaponized the Web," *The Guardian*, December 2, 2017, https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia.
[14] John R. Haines. Russia's Use of Disinformation in the Ukraine Conflict. February 17, 2015. Foreign Policy Research Institute. https://www.fpri.org/article/2015/02/russias-use-of-disinformation-in-the-ukraine-conflict/
[15] Hans Graf Huyn (1984). "Webs of Soviet Disinformation." *Strategic Review.* XXI:4, p. 52.
[16] *Wikipedia Online Encyclopedia*, "Active Measures," Last Edited March 24, 2017, https://en.wikipedia.org/wiki/Active_measures
[17] "Senate Intelligence Committee on the policy response to Russian interference in the 2016 elections: Victoria Nuland testimony," C-SPAN video, June 20, 2018, 1:29:27, accessed July 19, 2018. https://www.c-span.org/video/?447328-1/obama-administration-officials-testify-russia-election-interference.
[18] House Permanent Select Committee on Intelligence, Report on Russian Active Measures, March 22, 2018 https://fas.org/irp/congress/2018_rpt/hpsci-final.pdf./
[19] US Army Report on Russian Information Warfare. *Warfare.Today*, March 20, 2018, http://www.warfare.today/2018/03/20/us-army-report-on-russian-information-warfare/
[20] Wikipedia Online Encyclopedia, "*Disinformation*," Last Edited October 2, 2018, https://en.wikipedia.org/wiki/Disinformation
[21] Ibid.
[22] Leonard Doob. "Goebbels' Principles of Nazi Propaganda". *The Public Opinion Quarterly*. vol. 14, no. 3: 425.

[23] Estonian Foreign Intelligence Service, *International Security and Estonia*, Estonian Government public report, 2018, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf
[24] Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger, *"Countering Russian Social Media Influence"*, RAND Corporation, 2018, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf
[25] Molly K. McKew, "The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare. And it's probably being used on you," *Politico Magazine*, September-October 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538
[26] Timur Chabuk and Adam Jonas. "Understanding Russian Information Operations." *Signal AFCEA Magazine*, September 1, 2018, https://www.afcea.org/content/understanding-russian-information-operations
[27] Ibid
[28] There have been many active measures disinformation campaigns conducted by Russia against the US to include the following:

- Discrediting of the CIA, using historian Philip Agee (codenamed PONT).
- Stirring up racial tensions in the United States by mailing bogus letters from the Ku Klux Klan, placing an explosive package in "the Negro section of New York" (operation PANDORA), and spreading conspiracy theories that Martin Luther King, Jr.'s assassination had been planned by the US government
- Starting rumors that fluoridated drinking water was in fact a plot by the US government to affect population control
- Starting rumors that the moon landings were hoaxes and the money ostensibly used by NASA was in actuality used by the CIA
- Use of sympathetic elements in the press to libel the Strategic Defense Initiative as an impractical "star wars" scheme
- Fabrication of the story that AIDS virus was manufactured by US scientists at Fort Detrick; the story was spread by Russian-born biologist Jakob Segal.

These notable campaigns were obtained through exposure in the Mitrokhin Archives released by MI5, British Intelligence to the Churchill Archives Centre at Churchill College for public research in 2014.
[29] NATO, "NATO Welcomes Opening of European Centre for Countering Hybrid Threats," Apr. 11, 2017, https://www.nato.int/cps/en/natohq/news_143143.htm.
[30] Dorthey Denning, "Tracing the sources of today's Russian cyberthreat," *The Conversation*, August 15, 2017, https://theconversation.com/tracing-the-sources-of-todays-russian-cyberthreat-81593
[31]Jakub Kalensky, "How the Kremlin Exploits a Crisis," *Disinfo Portal*, April 8, 2019, https://disinfoportal.org/how-the-kremlin-exploits-a-crisis/.
[32] Katerina Eve Matsa and Elisa Shearer. Pew Research Center. News Use Across Social Media Platforms 2018. September 10, 2018. http://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/
[33] Ibid.
[34] Elis Shearer and Jefferey Gottfried. Pew Research Center. News Use Across Social Media Platforms 2017. September 7, 2017. http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/
[35] U.S. House of Representatives, Permanent Select Committee on Intelligence. Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements. https://intelligence.house.gov/social-media-content/
[36] David Z. Morris, "'White is Black and Black is White.'A Russian Troll Tells His Story," Febreuary 18, 2018, http://fortune.com/2018/02/18/a-russian-troll-in-his-own-words/
[37] James Mattis, US Secretary of Defense, National Defense Strategy, Department of Defense, Washington D.C., 2017.
[38] Jonathan PayCheck, Personal interview with European Lead Foreign Area Officer at Department of State, Global Engagement Center personnel, 15 March, 2019.
[39] Daniel Kimmage, "DisinfoWeek Brussels 2019: Daniel Kimmage", Atlantic Council, March 12, 2019, YouTube video, https://www.youtube.com/watch?v=fPzKb23V750
[40] Jonathan PayCheck, Personal interview with European Lead Foreign Area Officer at Department of State, Global Engagement Center personnel, 15 March, 2019.
[41] Euronews, "Lithuania has a volunteer army fighting a war on the internet", September 28, 2017, https://www.euronews.com/2017/09/28/lithuania-has-a-volunteer-army-fighting-a-war-on-the-internet
[42] UNESCO, "Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training", https://en.unesco.org/fightfakenews

[43] "Estonia welcomes EU action plan for tackling disinformation", The Baltic Times, December 7, 2018, https://www.baltictimes.com/estonia_welcomes_eu_action_plan_for_tackling_disinformation/
[44] European Union External Action, "Questions and Answers about the East StratCom Task Force, May 12, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en
[45] Odessablog, "East Stratcom Task Force and the EUvsDisinfo Budget – Too much or too little", November 24, 2017, https://odessablog.wordpress.com/2017/11/24/east-stratcom-task-force-and-the-euvsdisinfo-budget-too-much-or-too-little/
[46] Issie Lapowsky, "The State Department's Fumbled Fight Against Russian Propaganda", Wired Magazine, November 22, 2017, https://www.wired.com/story/the-state-departments-fumbled-fight-against-russian-propaganda/
[47] Terry Thompson. 10 JAN 2019. Public Radio International. Countering Russian disinformation in the Baltic nations; way. https://www.pri.org/stories/2019-01-10/countering-russian-disinformation-baltic-nations-way
[48] National Defense Authorization Act 2017
[49] Brian Kenety. Radio Praha. 21 NOV 2018. Ex-East StratCom Task Force Stalwart Jakub Kalensky on EU Efforts vs Russian Disinformation. https://www.radio.cz/en/section/in-focus/ex-east-stratcom-task-force-stalwart-jakub-kalensky-on-eu-efforts-vs-russian-disinformation
[50] Philip Ewing. NPR. May 23, 2017. Russia's Election Meddling Part of Long History of 'Active Measures'. https://www.npr.org/2017/05/23/528500501/lies-forgery-and-skulduggery-the-long-history-of-active-measures
[51] Jonathan PayCheck, Personal interview with European Lead Foreign Area Officer at Department of State, Global Engagement Center personnel, 15 March, 2019.
[52] Ibid.

BIBLIOGRAPHY

Allen, T. S.; Moore, A. J. "Victory without Casualties: Russia's Information Operations." *Parameters: US Army War College Quarterly* 48, no. 1 (Spring 2018): 59-71, https://www.hsdl.org/?view&did=812849

Brooking, Emerson T.; Singer, P. W. *LikeWar: Weaponization of Social Media*. New York: Houghton Mifflin Harcourt Publishing Company, 2018. iBooks edition.

Cantwell, Douglas. "Hybrid Warfare: Aggression and Coercion in the Gray Zone." *American Society of International Law: Insights* 21, no. 14 (November 29, 2017), https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone

Duggan, Patrick Michael. "Strategic Development of Special Warfare in Cyberspace." *Joint Force Quarterly* 79, no. 4 (October 1, 2015): 46-53, http://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyberspace/

Gertz, Bill. *iWar: War and Peace in the Information Age.* New York: Threshold Editions, 2017. iBooks edition.

Giannetti, William. "A Duty to Warn: How to Help America Fight Back against Russian Disinformation." *Air & Space Power Journal* 31, no. 3 (Fall 2017): 95-104, https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-30_Issue-1/2018_1_04_giannetti_s_eng.pdf

Hayes, Richard E.; Wheatley, Gary. "Information Warfare and Deterrence." National Defense University Press Book, 1996. Strategic Forum. http://www.dodccrp.org/files/Wheatley_Deterrence.pdf

Iasiello, Emilio J. "Russia's Improved Information Operations: From Georgia to Crimea." *Parameters: US Army War College Quarterly* 47, no. 2 (Summer 2017), https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2017/8_Iasiello_RussiasImprovedInformationOperations.pdf

Kitfield, James. "NATO Ops Center Goes 24/7 To Counter Russians: Gen. Scaparrotti." *Breaking Defense.com*, October 1, 2018, https://breakingdefense.com/2018/10/nato-ops-center-goes-24-7-to-counter-russians-gen-scaparrotti/

Król, Aleksander. "Russian Information Warfare in the Baltic States — Resources and Aims." *The Warsaw Institute Review* (July 20, 2017), https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/

Murphy, Dennis M.; White, James F. "Propaganda: Can a Word Decide a War?" *Parameters: US Army War College Quarterly* 37, no. 14 (Autumn 2007): 15-27,

http://www.au.af.mil/au/awc/awcgate/parameters/murphywhite.pdf

Nelson, C. Richard. “War of Ideas: More Than Simple Deception.” *Army: Association of the US Army Magazine* 66, no. 9 (September 2016) 12-13, https://www.ausa.org/issues/army-magazine-vol-66-no-9-september-2016

Pacepa, Ion Mihai; Rychlak, Ronald J. “The Role of Dezinformatsiya in the Framing of Pius XII.” *New Oxford Review* (September 2016) https://www.newoxfordreview.org/documents/the-role-of-dezinformatsiya-in-the-framing-of-pius-xii/

United Kingdom Interim Report. *Russian influence in political campaigns.* UK Parliament, 2017. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm