**APUS Library Capstone Submission Form**

This Capstone has been approved for submission to and review and publication by the APUS Library.

<table>
<thead>
<tr>
<th>Student Name</th>
<th>Clineard</th>
<th>Matthew</th>
<th>Evan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Number</td>
<td>INTL 699</td>
<td>Paper Date</td>
<td>December 2017</td>
</tr>
<tr>
<td>Professor Name</td>
<td>Redding, Robert W.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program Name</td>
<td>Intelligence Studies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capstone Type</td>
<td>Capstone-Thesis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passed with Distinction</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Sensitive Information</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRB Review Required</td>
<td>N</td>
<td>If YES, include IRB documents in submission attachments.</td>
<td></td>
</tr>
<tr>
<td>Turnitin Check</td>
<td>Y</td>
<td>All capstone papers must be checked via Turnitin.</td>
<td></td>
</tr>
</tbody>
</table>

* Required

**Capstone Approval Document**

The Capstone thesis/project for the master’s degree submitted by the student listed (above) under this title *

**IDENTIFYING AND CHARACTERIZING RUSSIAN DISINFORMATION**

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

<table>
<thead>
<tr>
<th>Program Representatives</th>
<th>Signatures</th>
<th>Date (mm/dd/yyyy)</th>
</tr>
</thead>
</table>
| Signed, 1st Reader * [Capstone professor] | Robert Redding | Digitally signed by Robert Redding
 Date: 2017.12.04
 12:27:28 -07'00' |
| Signed, 2nd Reader (if required by program) | | |
| Recommendation accepted on behalf of the program director * | | |
| Approved by academic dean * | | |

* Required

**Send Capstone submission to:**

ThesisCapstoneSubmission@apus.edu

**Attachments must include:**
- This completed form
- FINAL Capstone Thesis/Project document as Microsoft Word file
- IRB Review docs (if applicable)
IDENTIFYING AND CHARACTERIZING RUSSIAN DISINFORMATION

A Master Thesis

Submitted to the Faculty

of

American Public University System

by

Matthew Evan Clinard

In Partial Fulfillment of the

Requirement for the Degree

of

Master of Arts

November 2017

American Public University System

Charles Town, WV
The author hereby grants the American Public University System the right to display these contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by United States copyright law for the inclusion of any materials that are not the author’s creation or in the public domain.

© Copyright 2017 by Matthew Clinard

All rights reserved.
DEDICATION

I dedicate this thesis to my parents, Bob and Paula, and my Fiancé, Evaleen. It is through their constant love and support that I am able to pursue my dreams.
ACKNOWLEDGMENTS

I wish to thank the members of my faculty for their support. Dr. Robert Redding has been a valuable professor through the thesis process and has provided me the much-needed guidance and support throughout the course. I would like to personally thank him for this support as I worked through a difficult topic and finished out my degree.

Overall, I have found my course work throughout the Intelligence Studies program to be stimulating and thoughtful, providing me with the tools with which to explore both past and present ideas and issues.
ABSTRACT OF THE THESIS

IDENTIFYING AND CHARACTERIZING RUSSIAN DISINFORMATION

By

Matthew Evan Clinard

American Public University System, 5 November, 2017

Charles Town, West Virginia

Professor Robert Redding, Thesis Professor

The purpose of this research was to identify key characteristics and tactics of Russian disinformation operations. By examining several case studies through content analysis and by conducting a Qualitative Comparative Approach (QCA), this research found that the most common tactics used by the Russian disinformation apparatus included: a targeted media campaign, social media as a tool, trolls on social media sites, fake news stories, and fake interviews. Additionally, this research found that the most common environmental variables that make Russian disinformation likely included: a target nation that was a former Soviet territory, a Russian speaking population, a nation with policies that lean towards the West, is a NATO member, borders Russia, and has access to Russian media broadcasts within their media architecture. In conclusion, this research has provided the groundwork, as well as, a central
source of information regarding Russian disinformation operations that will allow future operations to be identified, further research to be completed in specific geographic areas, and the growth of information operations to counter Russian disinformation. Lastly, this study has also identify countries like Poland and Georgia as potentially vulnerable areas to Russian disinformation, based solely on the variables that create a fertile ground for Russian disinformation.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td></td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II.</td>
<td></td>
</tr>
<tr>
<td>LITERATURE REVIEW</td>
<td>5</td>
</tr>
<tr>
<td>Western Populations are the Target</td>
<td>7</td>
</tr>
<tr>
<td>Domestic Population is the Target</td>
<td>10</td>
</tr>
<tr>
<td>General Information Operations</td>
<td>13</td>
</tr>
<tr>
<td>New War Theory</td>
<td>14</td>
</tr>
<tr>
<td>Conclusion</td>
<td>16</td>
</tr>
<tr>
<td>III.</td>
<td></td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>18</td>
</tr>
<tr>
<td>Setting</td>
<td>18</td>
</tr>
<tr>
<td>Sample</td>
<td>19</td>
</tr>
<tr>
<td>Materials</td>
<td>20</td>
</tr>
<tr>
<td>Measurement Instruments</td>
<td>21</td>
</tr>
<tr>
<td>Data Collection/Procedures</td>
<td>21</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>21</td>
</tr>
<tr>
<td>IV.</td>
<td></td>
</tr>
<tr>
<td>FINDINGS &amp; ANALYSIS</td>
<td>23</td>
</tr>
<tr>
<td>Content Analysis</td>
<td>23</td>
</tr>
<tr>
<td>Sweden and Finland Case Study</td>
<td>23</td>
</tr>
</tbody>
</table>
Baltic Nations Case Study.................................................................27
Ukraine Case Study .................................................................29
Crimean Peninsula Case Study.....................................................30
General Disinformation Operations..............................................33
Syria Case Study......................................................................36
Commonalities.........................................................................37
QCA Structure........................................................................41
Computations..........................................................................43
Analysis..................................................................................48

V. CONCLUSION........................................................................51

LIST OF REFERENCES.............................................................53
LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Table 1. All positive and Negative Cases with Truth Values</td>
<td>43</td>
</tr>
<tr>
<td>2. Table 2. All Positive and Logically Consistent Cases</td>
<td>44</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURES</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Figure 1. Complex Solution to the csQCA</td>
<td>46</td>
</tr>
<tr>
<td>2. Figure 2. Parsimonious Solution to the csQCA</td>
<td>47</td>
</tr>
<tr>
<td>3. Figure 3. Intermediate Solution to the csQCA</td>
<td>48</td>
</tr>
</tbody>
</table>
CHAPTER ONE
INTRODUCTION

In the middle to late 1990’s, the world was recovering from a decades long Cold War between the Soviet Union and the West. The Soviet Union, now the Russian Federation, was reeling from an economic collapse, a massive change in government, and was suffering from somewhat of an identity crisis. As Pranas Ciziunas points out, “…overnight in 1991, the power of the Soviet Union, and therefore of Russia, disappeared, leaving the country suffering from what is called a greatness syndrome…” (Ciziunas 2008, 287). During the nineties, Russia struggled to rebuild their image and standing in the world, but continued to make a slow progress in a positive direction. It took roughly two decades for them to recover from this apparent crisis and gain a foothold back on the world stage, and they have done so in spectacular fashion. In 2008, Russia invaded the sovereign territory of Georgia and essentially annexed the territories of Abkhazia and South Ossetia. In 2014, Russian forces moved into Crimea and set the stage for a referendum that allowed Russia to annex the Crimean Peninsula. Then, later that year, under the guise of Ukrainian separatists, forces moved into Eastern Ukraine and have effectively fought to a stalemate. The regions of Donetsk and Luhansk have been under Russian control and influence ever since, and the fighting continues. Lastly, in 2015, Russia moved additional forces into Syria and have joined the complicated web of forces fighting for power and territory in Syria. With those major events, Russia has forced itself back into the international conversation. They have made themselves a major player in affairs around the world, and have reestablished their image as a nation not to be meddled with. In combination with the actions in Georgia, Ukraine and Syria there has been a massive increase in propaganda in the form of media and internet disinformation. During each of those conflicts the Russian media played a major role in spinning
the events in a positive light using themes like “the fall of the Soviet Union was a disaster of global proportions” (Kofman et al. 2017, 81). Additionally:

Russia has invested immense resources into applying the tools of globalization to a massive program of disinformation. It has combined nationalism within Russia, with the legend of a proud nation humbled by the evil West and added an extra dose of old fashioned anti-Americanism to shoot an unbroken stream of invective around the world (Kornblum 2015, 8).

Romanian author Anton Bebler analyzed the type of propaganda used during the annexation of Crimea, saying “President Vladimir Putin and official Russian propaganda used the right of the Crimean people to self-determination in the form of secession as the chief argument to justify and legitimize the annexation” (Bebler 2015, 45). This use of state-controlled media and overwhelming disinformation harkens back to the day of Soviet use of “active measures” as a controlling mechanism for their area of influence. “Active measure,” the term used to describe the use of soft power influencers, such as propaganda, TV outlets, and newspapers, has been described by DeWitt Copp as “…a spectrum of white (overt), grey (semi covert), and black (covert) operations (DeWitt 1996, 155). However, these tactics have now been updated for the 21st century. In fact, it was noted as early as 1995 by a prominent Russia military theorist that “…countries could ‘become objects of information warfare.’ He speculated that the opening stages of a war would feature disinformation campaigns whereby belligerents would seek to undermine local trust in the governments they targeted” (Lanoszka 2016, 188). Depending on the source, Russian soft power influencers are sometimes described as hybrid warfare, information operations, or disinformation tactics. The biggest difference now, compared to the Soviet days, is the use of a globally interconnected internet and 24/7 news broadcast networks.
Those global reaching services in combination with people, or secretive forces, on the ground are used to push the Russian agenda. With that in mind, this research study will analyze this recent trend in the context of New War Theory. New War Theory examines modern day conflicts in terms of conflicts of identity and groups as opposed to the traditional Clausewitz view of war that examined conflict between states and governments.

The difficulty in trying to understand when and how disinformation tactics are being utilized is due to the very nature of these measures being secretive and deceptive. As Michael Mihalka points out in describing strategic deception that “often statesmen disguise their true intent from others and memoirs after the fact often betray greater vision than the confusion of the actual moment suggested. Actual plans or programs for deception should have limited circulation and thus should rarely enter the public domain” (Mihalka 1982, 40). Utilizing a little background in disinformation, however, such as that provided by David Rothkopf in *The Disinformation Age*, and the analysis of recent events in Europe, this paper compiles a series of European case studies that identify key indicators and characteristics of Russian disinformation into an easily digestible summary of Russian activity. While Russian soft power influencers, or more specifically disinformation tactics, have been used around the world in support of Russian forces and political interests, there has been a large use of these tactics in Europe. In particular, the use of disinformation tactics was utilized throughout the previously mentioned conflicts and continue to be used throughout major parts of the European continent. To help focus the content, the scope of this research will only cover the use of disinformation tactics within the eastern part of Europe, but will ideally apply to the use of similar tactics across the world. This paper also examines the environmental factors, or variables, that provide the setting used for Russian disinformation campaigns. The overall purpose of this paper is to provide a deeper understanding
of Russian disinformation operations and an analytical backbone from which one could perform further analysis of disinformation tactics utilized by the Russian government. By building a structure to analyze the scale of the operations and the key indicators of disinformation operations, it will ideally allow a more targeted approach to countering Russian influence in terms of Western attempts to mitigate Russian influence. Ultimately, the question answered by this paper is: what are the key characteristics and indicators that can be used to identify Russian disinformation operations?
CHAPTER TWO

LITERATURE REVIEW

Before diving into a review of the literature, it is important to reiterate exactly what this paper will be focusing on for the remainder of the discussion. As Russia began to figuratively and literally march their forces back into Europe, as they began to force themselves back onto the world stage, and as the atmosphere and environment around Europe began to shift, Russia was conducting disinformation in full force. As this paper describes, this included a wide variety of tactics that were conducted in the cyber realm, the media realm, and on social media. An important thing to highlight, however, is that a majority of the disinformation tactics that were witnessed during the last three years were used either domestically to Russia, or within their closest reach (i.e. eastern and central Europe). These nations have recognized the threat and have made great strides to try and combat the overflow of fake news articles, falsified media reports, and targeted social media trolling. For example, Jaomiasa Handy Francine points out in her article “European Union in the age of misleading communications: Insights on disinformation and propaganda” that the European Union has established a task force designed to identify and counter disinformation tactics used against their subordinate nations. She says “Called the East StratCom Task Force [the European Union] set up [the task force] following the European Council in March 2015, which tasked the High Representative to submit, in cooperation with EU institutions and Member States, an action plan on strategic communication in order to address Russia’s ongoing disinformation campaigns” (Handy 2016, 39). It is in this context that this research paper examined certain European case studies and the necessary secondary sources to clearly lay out what the disinformation tactics look like.
Additionally, it is important to identify and define some of the key terms that have already been introduced in the introduction and that will be used throughout the rest of this paper. When talking about Russian disinformation, many of the sources used the terms disinformation, information operations, and misinformation. Therefore, this paper will use those same terms interchangeably, but all to mean Russian disinformation and the associated tactics. Additionally, the terms tactics, operations, and campaigns are also used significantly throughout the paper and meant to represent the use of tools and procedures by the Russian government to spread disinformation. Throughout the paper, the words will be used to describe either a specific type of technique, or the whole of tactics being used against a targeted audience.

Moving forward, an initial look at the literature shows that it is indeed difficult to determine exactly when and how the Russian government uses disinformation. A majority of the literature that has been examined thus far primarily addresses disinformation and media campaigns as part of a larger story. A few of the articles simply mention the use of certain disinformation tactics, while others dive a little deeper into the specifics and give quantified information regarding the employment of tactics. For example, the article by Martin Kragh and Sebastian Åsberg attempts to break down major themes and tactics used by Russian media targeting the Swedish population over the course of 2015. They examined 3963 articles from the Swedish language version of Sputnik in order to detail the goals of Russian disinformation, concluding that “the overarching goal of Russian policy towards Sweden and the wider Baltic Sea is to preserve the geostrategic status quo, which is identified with a security order minimizing NATO presence in the region” (Kragh and Åsberg 2017, 36). All in all, there are a couple major themes that stand out amongst all the literature. The first major theme is the use of disinformation tactics to push specific geopolitical narratives to the domestic population of
Russia. This ranges from bolstering Russian nationalism to providing false accounts of events taking place around the world. The second major theme is the use of disinformation tactics to push stories, narratives, and ideas out to the western world to try and change the West’s perception of events. While these topics are separated into distinct categories within the literature review, that does not necessarily mean that the ideas and tactics described in the literature are mutually exclusive. In fact, this research has found quite the opposite. What that means is that there are commonalities between the two previously mentioned themes which ultimately add up to a complete picture of Russian disinformation tactics. On top of all that, this paper will examine these tactics in the context of New War Theory in order to address the overarching ideas that drive the operations. Therefore, this literature review will include a discussion of New War Theory and how Russian disinformation fits into this new model within the international relations community. Lastly, to gain a better understanding on information operations as a whole, this literature review will also examine some basics of information operations, look at the growth of operations as the internet was coming online, so to speak, and see how the use of global reaching communications has been a concern for some time.

**Western Populations are the Target**

The first major theme exhibited in the reference articles is that Russia is actively controlling information disseminated amongst a target populations outside its borders in order to influence those populations. A good example of this is demonstrated in “Crimea and the Russian-Ukrainian Conflict” by Anton Bebler who describes the use of media and disinformation by the Russian government during the ongoing conflict in Ukraine. He says Russia’s goal through the media was to isolate the population from outside media sources and increase propaganda within the target population, to include the shutdown of Ukrainian TV stations in the
occupied territory of Crimea and the controlled dissemination of printer newspapers. He states “The population of Crimea was thus subjected to one-sided information and often outright disinformation by the Russian state-controlled mass media” (Bebler 2015, 42). Throughout the rest of the article, Bebler provides a detailed analysis of the tactics used by Russian forces on the ground to control the information being released to the target population on Crimea. Overall, this article has proven to be a great resource for the analysis later in this paper.

Similar ideas are potentially being employed in the Baltic states as well, which has been described by Pranas Ciziunas in “Russia and the Baltic States: Is Russian Imperialism Dead?” as well as by Andrew Radin in his article *Hybrid Warfare in the Baltics*. Ciziunas describes the situation saying that mostly Russian media outlets are utilized to project specific messaging and disinformation. For example, he describes the tactic of using western commenters speaking out against the targeted population saying “…such information campaigns attempted to discredit the Baltic governments and their supporters” (Ciziunas 2008, 290). Similarly, Radin claims that more money is spent on production for Russian language media in target areas, providing disinformation about current events around the populace and the government’s overall goals. He says “many observers also note that products on Russian media generally have significantly higher production values than locally produced shows, and… Russian television in particular is easier and more enjoyable to watch.” (Radin 2017, 18). Overall, at this point, it is already clear that there is a significant and complex planning process that goes into creating the right messaging for the Russian government. Both of these articles provide credible details and assessment regarding the use of Russian disinformation capabilities in a future conflict. This was extremely useful when crafting the summary of Russian disinformation tactics.

Another major example of Russian disinformation attempts comes from the article
“Russia’s strategy for influence through public diplomacy and active measures: the Swedish case” by Martin Kragh and Sebastian Åsberg. The situation is described as troll armies targeting media members and hijacking twitter, the spreading of fake news on Russian media sources (which is subsequently picked up by some Swedish news sources), and the use of categorized themes of articles, or fake news stories on social media. The Swedish authors provide us some details on specific tactics being utilized, describe previously in the introduction, which was extremely beneficial for breaking down the types and quantity of tactics being utilized by the Russian government for their targeting disinformation campaign. While this article focuses squarely on the effects of disinformation on the Swedish population, it nonetheless provided the details and descriptions necessary to carry out the research.

Next, Vince Houghton interviews a former RT news anchor, Liz Wahl, in the podcast that he hosts called SpyCast. In the episode, titled “Dezinformatsiya,” Liz Wahl describes the not so subtle campaign to influence US public. RT, discussed in the podcast, is a major English speaking media organization that is controlled by Russian masterminds, whose intent is to discount the West and provide a medium for disinformation and fake news. The episode dives into the use of targeted social media posts and news stories, as well as, the purposeful publishing of fake news in order to achieve a couple different objectives: add confusion to events that currently happening on the ground and inject fake stories to discredit an organization, a group, or even a nation. This is another great example of a tactic used by the Russian state media, however, it is a single biased person’s account of the events. Anything reported on this podcast will have to be taken less academically.

Lastly Christopher Chivvis in “Understanding Russian ‘Hybrid Warfare’: And What Can Be Done About it,” and Bruce McClintock in “Russian Information Warfare: A Reality That
Needs a Response” discuss the common trend of disinformation tactics used to target western nations. Chivvis says “[Using hybrid measures to influence the politics and policies of countries in the West and elsewhere] seeks to ensure that political outcomes in targeted countries serve Russia’s national interests (Chivvis 2017, 3). Chivvis points out that one of the major tenants of Russian Disinformation operations is to influence the populations outside of its domestic realm. This is important to understand because, as mentioned before, certain types of tactics might be used against a different population target. It was the further analysis of these details that revealed more of the complete answer. 

Overall, there are several strong cases for the use of disinformation operations to target outside populations to push the Russian policy agenda. In addition to that, there are several sources that provide great detail about the specific tactics utilized and perceived during these information operations. However, as closer look at target disinformation in the domestic sphere reveals some similarities.

**Domestic Population is the Target**

The second major theme presented throughout some of the articles is that the target of Russian disinformation is actually primarily the domestic population. Michael Kofman et al. in their article *Lessons from Russia’s operation in Crimea and Eastern Ukraine*, as well as, Arkady Ostrovsky in his book *The Invention of Russia: The Rise of Putin and the Age of Fake News* describe the Russian government effort to sway the domestic population in a similar way as described above. They both discuss the use of themes that are present in the stories, reports, articles, and interviews that are pro-Russian in nature and are similar throughout topics and news sources. Ostrovsky describes the situation in Ukraine saying “…never before had wars been conducted and territory gained primarily by means of television and propaganda” (Ostrovsky
Additionally, they both discuss specific tactics utilized by the Russian state-run media companies, to include: actors, doctoring quotes, using fake footage, and social media trolls. Both will provide excellent data to include in the overall study, as well as, specifics regarding tactics utilized during the campaigns and the domestic targets. The biggest concern about Ostrovsky as a source is that he has a severe bias leaning away from Russia and might have a skewed perspective. However, his overall argument is laid out clearly and convincingly. Kofman et al provides a solid objective and analytical view of the conflict and was used to back up Ostrovsky’s account.

Backing up Kofman and Ostrovsky is Christopher Paul with his article *Firehose of Falsehood*. According to Paul, common tactics within the Russian disinformation apparatus include the recycling of disinformation, the use of actors, fake on-scene reporting, and manufactured sources. He states “Contemporary Russian propaganda is continuous and very responsive to events… [Russian propagandists] just disseminate an interpretation of emergent events that appears to best favor their themes and objectives” (Paul 2016, 4). This falls exactly in line with the information being described by both Kofman and Ostrovsky in the previous two sources, and further adds to the bulk of data.

Similarly, Dmitry Shibaev and Nina Uibo, in their article “State Policy Against Information War” describe the “information wave” as a tactic used in disinformation campaigns. This information wave is effective when refutation is published with reference to an expert, a politician and public figure, publishing house, organization, etc. Following that, “the third or fourth reprints of the information are sure to be indexed on behalf of this expert or politician and public figure or publishing house” (Shibaev and Uibo 2016, 148). Overall, the same concept described by Paul in his article is also being described by these two Russian lawyers. Clearly,
these sources are on to something that is becoming a trending tactic. As a source, this one in particular provides some bias that is opposite of the majority of the rest of the sources and provides some balancing in the whole effort.

In his book *Nothing is True and Everything is Possible*, Peter Pomerantsev discusses how the spreading of Russian themes of supremacy and overall information operations have done their job. Additionally, Pomerantsev describes how, to a large pool of the population in Russia, the nation and story of Russia means a lot to a great deal people. However, along with that narrative being pushed by Russian media outlets is the idea that everyone else outside of the Russian population is a bad guy. He describes a scenario saying “the West, [a Russian news presenter] will say, is sponsoring anti-Russian ‘fascists’ in Ukraine, and all of them are out to get Russia ad take away its oil…” (Pomerantsev 2014, 230). This type of scenario fall right in line with the type of tactics and themes that have already been identified in the previous articles. The Kremlin creates, modifies, and manipulates stories all to their advantage, using tools like RT to broadcast their narrative. Similar to Ostrovsky, there are some inherent biases that have to be contended with, however, Pomerantsev provides some needed inside context for the use of disinformation and the effects of the tactics.

The last article that falls in line with the rest is *Putin’s Propaganda Machine: Soft Power and Russian Foreign Policy* by Marcel Van Herpen. Russian information operations come from Russia’s policy designed to increase its soft power. According to Van Herpen, there are three components to Russia’s soft power information campaign: mimesis, rollback, and invention. It is the third component of this soft power apparatus that we see the use of disinformation campaigns, and as Van Herpen describes is “…a large-scale, centrally led and coordinated effort by the Russian state with the aim of creating the maximum possible impact”
What makes this article slightly different than the rest is that Van Herpen describes the situation saying that the information campaign can be and is used outside the domestic Russian populace to target western nations. However, his overall conclusion is that the disinformation tactics used are primarily focused on the internal populace.

In all, while the focus of these articles describes the use of disinformation tactics to influence the domestic Russian population, there are some consistent themes throughout both topics. The use of similar fake news, propaganda style tactics to influence a targeted audience is common throughout, but the specifics are broken out in the overall analysis.

**General Information Operations**

While the previous two topics generally summarize the bulk of the answers needed to answer the research question, a discussion on Russian disinformation requires some context in the greater growth of information operations around the world to make historical sense.

To start, David Rothkopf in “The Disinformation Age” provides a solid context for the growth of the information age and the use of information technologies to the advantage of an actor. He states “…information technology is only as good as the information it delivers, and the flow of information is compromised at many levels” (Rothkopf 1999, 83). This description provides an ominous tale of how information being passed through technology of the digital age can be and is manipulated as it moves from person to person, organization to organization, and state to state. This is important to understand because it provides the background necessary to understand how information operations have been integrated into a greater government policy strategy, and in the case of Russia its policy and military strategy.

Speaking to the military integration of information operations and disinformation tactics, Col James McLendon, in his article “Information Warfare: Impacts and Concerns,” describes
how information warfare has become the new 4th dimension of conflict. As he lays out, information warfare helps to shape the battlespace to the advantage of the aggressor. Interestingly enough, he points out that the Russian generals already recognized this back when this was published in 1998. He states “Russian senior military officials have already recognized the integration of information technology ‘could generate radical use of intellectualized weapons in the organizational principles of armed forces’” (McLendon 1998, 191). What this tells the reader and what this adds to the research is that the Russian’s have been looking at this type of warfare for at least two decades already. The first real use of this type of warfare in a conflict is expertly described by Inga Von der Stein in her article The Media as an Instrument of Information Warfare. The article takes a quantitative look at propaganda in European and Russian newspapers during the Russian-Georgia conflict a decade ago and concludes that the Russian disinformation campaign was in full swing during conflict. Not only does this provide the context for how we arrived at the current situation, but provides additional details regarding the use of disinformation to target a specific outside populace.

Lastly, George Stein, in his article “Information War – Cyber – Net War,” defines information warfare and Net War for the reader and is definitely of value for this overall research. Ultimately he provides an evaluation of the US’ current and future ability to project an influence campaign and also defend against disinformation operations. What he concludes is that we need to seriously restructure our capabilities. While this does not add any direct progress towards answering the proposed research question, it does provide some additional context for the current state of affairs.

New War Theory

In order to narrow the focus of the research conducted in this study, any and all research
will be placed in the context of an international relations theory known as New War Theory. New War Theory has been proposed by Mary Kaldor and argues “…that contemporary types of warfare are distinct from the classic modern forms of warfare based on nation-states” (irtheory.com). According to Kaldor, “New wars are fought in the name of identity (ethnic, religious or tribal) …The aim is to gain access to the state for particular groups (that may be both local and transnational) rather than to carry out particular policies or programs in the broader public interest” (Kaldor 2013, 2). Additionally, new wars depend less on military violence to capture territory, but instead “battles are rare and territory is captured through political means, through control of the population” (Kaldor 2013, 2). Ultimately, this means that information operations, and in this case disinformation campaigns, are a likely tactic utilized in these new war type conflicts. The target audience is an important variable in identifying the use of specific tactics, as well as, the tactics themselves.

In contrast to Mary Kaldor, Bart Schuurman argues for a close examination of the New War Theory compared to previous views of warfare in his article “Clausewitz and the ‘New Wars’ Scholars.” He says that New War scholars tend to dismiss Clausewitz as a way of viewing old, state-on-state conflicts, and that with new war, Clausewitz no longer applies. However, he argues, Clausewitz is not solely state-on-state and is just as relevant today as he was previously. He says “the trinity [violence, chance, and rational purpose] elegantly rejects the notion of distinct historical phases by showing how the variable relationship between three ever-present elements can account for an unlimited variation of conflicts that are given their particular shape by contextual specifics (Schuurman 2010, 98). What he is implying is that Clausewitz’s theory is flexible enough to make sense, even in modern wars like the current War on Terrorism. New War Theory, as Schuurman claims, only adds to the confusion about how to interpret, analyze,
and move forward in finding solutions to complex wars like that against global terrorism. It is a great point worth considering and provides another way of analyzing a situation, like that of Russian disinformation. However, New War Theory still provides the correct context based on the observed objectives of Russian disinformation, namely the targeting of populations for a specific gain.

**Conclusion**

In conclusion, there is a plethora of research that has been conducted to document the existence of Russian disinformation operations. Several case studies have been completed that look at tactics used, the end state of the Russian disinformation, or at the very least the potential outcomes. Within that variety of sources are two major themes: the target population of Russian disinformation tactics is the domestic Russian population, and the target population is outside people, groups, and nations. The intent in both cases being to influence the population towards Russian ideals, themes, and goals. While the individual sources provided great context and descriptions for the type of tactics utilized by the Russian government, there were some fairly consistent themes that ran through both topics. One is that there is a complex, full-force apparatus behind the disinformation campaigns with specific goals and intents. The tactics utilized are meant to portray either a pro-Russian theme, or an anti-West theme for both audiences. Additionally, the tactics utilized in both cases are similar and consist of: fake news on major media outlets, the use of bots and trolls on social media, the controlled dissemination of information to the target population, and the use of actors, sets, and mock-interviews to produce confusion in a data rich environment.

Additionally, several of the sources discussed provide the right context in which this research paper analyzed the situation. The Russian military and government has been looking at
the growth of the information age and information technology with the intent of incorporating its use into their greater grand strategy. The biggest difference between current Russian information operations and old soviet tactics is the extensive use of that massive amount of information age technology and the combination of that with military objectives on the ground. All of that ultimately fits into the mold of, and adds an ever-growing example of how 21st century warfare is based more on the population as the target. This is best described by New War Theory and its analysis of current conflicts with the idea that big military objectives are less likely in the globalized society that we live in today.

With all that being said, no study has combined these case studies to examine for specific tactics and characteristics that are distinct to Russian disinformation operations. Once these techniques have been analyzed, they will ideally provide the context for future studies to develop methods to determine near-real-time when disinformation campaigns are in full effect, as well as, identify potential counters to the known tactics and strategies.
CHAPTER THREE

METHODOLOGY

Looking at the growth of Russian influence on the international stage over the last decade, disinformation operations have become a major factor in understanding intent, objectives, and precursors to major geopolitical situations with regards to Russia. As discussed already in the introduction to this paper, as well as, the literature review of previously published academic work there is a lot of good information that exists regarding the specific tactics and relative effects of Russian disinformation operations. However, as previously mentioned, there has been little to no work done to organize the multitude of case studies into a combined research project that analyzes the existing data for patterns, themes, and similarities that can be used to identify Russian disinformation operations in the future. As discussed, the question answered by this paper is: what are the key characteristics and indicators that can be used to identify Russian disinformation operations? The following sections describe, explain how, and with what data this research project will use to answer that question.

Setting

To start, it is important to understand the setting for which the research study took place. This study did not take place in a specific location, or with a focus on a specific area, nor did it examine primary sources and raw data (which will be discussed later). Instead, it examined case studies for several different areas of operation to include: Sweden, Finland, the Baltics, Crimea, Ukraine, Syria, and the use of disinformation tactics in general. These case studies provide a varying degree of observed disinformation operations and tactics, and allows for the identification of different patterns and themes that are common through the different area of operations. By conducting the study this way, it allows for the discovery of the specific answers
Sample

Next, this study used secondary qualitative research as the primary type of research. Given the limited time and resources available to complete this study, the use of already available data was the best way to move forward. Identifying, tracking, and counting disinformation tactics down to the individual fake news article, staged interview, or twitter bot is a very time intensive and resource consuming undertaking. With that in mind, there are a plethora of case studies that have already been completed that have already done a majority of that leg work. The use of those individual case studies allowed this research project to conduct the necessary secondary research and to pull the necessary data to answer the overall research question. Additionally, combining those case studies provided the necessary data across multiple area of operations needed to analyze the different tactics and themes utilized by the Russian government during their disinformation operations.

While there are different methods when it comes to carrying out primary or secondary qualitative research, since this study is using entirely secondary resources the main method of research is content analysis. Content analysis can be described as a “set of methods for analyzing the symbolic content of any communication” (Singleton and Straits 2010, 420). Similarly, content analysis as a tool provides “a set of procedures for collecting and organizing nonstructured information into a standardized format that allows one to make inferences about the characteristics and meaning of written and otherwise recorded material” (USGAO 1991, 102). The analysis of the case studies, or published documents, is non-intrusive, allows the examination of previously collected data, and provides a historical insight into the use of disinformation tactics by the Russian government. This insight provides clues into the overall
intent, but more specifically what kind of tactics have been utilized in specific scenarios. It is the next step of the research process that this paper uses that brings those case studies together to examine for patterns and conditions.

**Materials**

In order to complete the research and analysis required to answer the question there are several different materials that are required. First and foremost, one of the primary tools is the book *Coding Manual for Qualitative Researchers* by Johnny Saldaña. This resource provides the method for which the qualitative information in the different case studies examined can be coded, so that it can be examined in the process described below. Saldaña quotes C. Grbich saying “when you apply and reapply codes to qualitative data, you are codifying – a process that permits data to be divided, grouped, reorganized, and linked in order to consolidate meaning and develop explanation” (Saldaña 2016, 9). What that means for this study is that the words, tactics, and qualitative information described in the case studies can be turned into a rough quantitative data set that can then be analyzed for patterns and conditions.

On top of that, the website Compasss.org is one more important item required to complete this study. This website provides downloads of analysis software which allow the coded qualitative information that has been organized in the analysis model described below to be examined for patterns and themes. Therefore, instead of the individual person having to examine the quantified data for patterns, a software algorithm will run through the numbers and identify patterns and themes based on user inputs.

**Measurement Instruments**

For the actual analysis of the data, this study uses a process called QCA which is the primary research tool that helped answer the proposed question. QCA “…is a method that
bridges qualitative and quantitative analysis” (Ragin 2008, 3), and provided this study the necessary answers to arrive at a reasonable analysis and conclusion that allows further research to be completed. It is an important tool because it: allows for the examination of qualitative information in a pseudo-quantitative way, allows for the study of a smaller number of cases than what could be examined statistically, and it does not require the same assumptions that statistical analysis requires. Additionally, “using QCA it is possible to assess causation that is very complex, involving different combinations of causal conditions capable of generating the same outcome” (Ragin 2008, 3). This is the ideal toolset necessary to pluck patterns and conditions out of individual complex scenarios with a limited number of data points.

**Data Collection/Procedures**

In order to complete the QCA, this paper uses case studies (i.e. Ukraine, Crimea, and Sweden) to fill out the data sets. This was done by recording the data from the several different case studies into one complete data set, as each individual case study has already compiled data for its specific region of disinformation operation. The data used includes, but is not limited to the presence Russian media, the intended audience, the country the information is presented within, and its membership in NATO. The data sets were divided by case study/region to keep the data organized. However, once the data was collected, it was coded and run through the QCA together in order to examine the information for conditions and patterns.

**Data Analysis**

Most of the analysis has been covered by the explanation of the materials and instruments that are used in this study, but there are some key points to consider. The data is primarily qualitative in nature, but there is some quantitative information available in each of the case studies. The quantitative data will be recorded in the overall data set, but the qualitative data will
be coded and recorded for analysis. The primary way the data was analyzed was through a QCA that was run through tools from compasss.org to identify patterns and themes.

As already mentioned, this study did not conduct its own primary data collection, but instead depended on already completed case studies in order to fill out the overall data set. With that, the potential biases associated with this research are based on the sources used. The view of tactics being utilized, the biased associated with observing the disinformation tactics, and the ability of the previous researchers to identify the tactics all play a role in the overall error associated with the study. However, by cross comparing the individual case studies, this study will ideally limit some of the biases, as well as, identify patterns and themes that are constant regardless of the ability of researchers to properly identify disinformation tactics to the individual iteration.
CHAPTER FOUR
FINDINGS & ANALYSIS

Content Analysis

While there exists a large body of academic information regarding Russia’s use of disinformation tactics, a majority of the work has been done in the context of specific situations. For example, there were several case studies completed by the RAND organization that analyzed and described the Russian involvement in Ukraine and Crimea. Additionally, studies have been done around Europe to include a look at Russian disinformation tactics in the Baltics, as well as, Finland and Sweden. This is not a new threat, which has been alluded too; in fact, the 1952 Great Soviet Encyclopedia called disinformation tactics the:

Dissemination (in the press, on the radio, etc.) of false reports intended to mislead public opinion and suggested that the Soviet Union was the target of such tactics from the West. In his book ‘Disinformation,’ Pacepa wrote that the Soviet manuals he read as a young intelligence officer described disinformation as a tactic used by Moscow with roots in Russian history (Taylor 2016, 1).

Overall the intent of this section is two-fold: first, to compile the relevant pieces from each of those individual case studies into one source, as well as, an easily digestible summary; second, to use the QCA techniques described above to take a look at the greater context behind Russian influence operations.

Sweden and Finland Case Studies

To start, the first case study examined for this research was a study done for Russian disinformation operations within the country of Sweden. This study, titled “Russia’s strategy for influence through public diplomacy and active measures: the Swedish case” by Martin Kragh
and Sebastian Åsberg, examined 3963 articles between April and December of 2015 in the Swedish language version of the Russian news organization Sputnik. Kragh and Åsberg examined those articles for what they called metanarratives, or overarching themes. Sputnik International created a Swedish language version on 15 April 2015 and was meant to target the Swedish speaking population of Sweden directly in order to direct specific messages and themes, as well as, to provide disinformation in an oversaturated world of media coverage. The two authors mention “Moscow is communicating to different target populations, but it remains to be properly understood exactly what is being said. The establishment of a Swedish language Sputnik news website in April 2015 was in this respect helpful” (Kragh, Martin and Sebastian Åsberg 2017, 3). What they are suggesting is that the creation of a Swedish language media outlet makes it very clear who the targeted audience was for the Russian disinformation operation. In this case, it was the external (to Russia) Swedish population.

From those articles, 3344 were categorized into ten categories, with the remaining 619 dismissed as outliers due to their miscellaneous character. Of those 3344 articles, the themes identified by the authors were: “Crisis in the West (705 articles), Positive image of Russia (643) and Western aggressiveness (499)...Negative image of countries perceived to be in the West’s sphere of influence (424), West is malicious (309), International sympathy and cooperation with Russia (304), Western policy failures (112) and Divisions within the Western alliance (72)” (Kragh, Martin and Sebastian Åsberg 2017, 10). Based on these identified categories, Kragh and Åsberg point out that “…the continuity with Soviet mass communication themes is very strong, with a general emphasis on anti-Western narratives” (Kragh, Martín and Sebastian Åsberg 2017, 10).

An initial breakdown of the tactics utilized by the Russian government for this specific
example of disinformation operations shows that they have chosen to use targeted media outlets as one way to communicate their message. Unlike other instances, Kragh and Åsberg point out that outright fabrications, or fake news stories, were limited in scope. In this case study, at least in the time period covered, there was limited use of that specific disinformation tactic. However, there was one prominent example of disinformation published through the Swedish version of Sputnik. This example was the “…counter-hypothesis supported by Russia that the civilian airliner MH17, which crashed in the Donbass region of Ukraine in July 2014, was shot down by a Ukrainian fighter jet rather than a surface-to-air missile operated from rebel held territory” (Kragh, Martin and Sebastian Åsberg 2017, 16).

Lastly, Kragh and Åsberg point out that “An increasing amount of disinformation, forged telegrams and fake news items have surfaced in the Swedish information landscape” (Kragh, Martin and Sebastian Åsberg 2017, 2). Therefore, in addition to the use of a targeted media campaign, the Russian government was also using other types of disinformation tactics throughout Sweden. In fact, the authors list examples such as pro-Kremlin non-governmental organizations (NGOs) and government-organized non-governmental organizations (GONGOs) have started operating in Sweden, there have been revelations of a Russian owned company in Sweden connected to party financing, troll armies have targeted journalists and academics, and Russian state TV has portrayed cases of fake interviews with Swedish citizens that chastise the Swedish government and the West. Unfortunately for those involved, not all of the Swedish citizens taking part in the spread of this disinformation are aware that they are acting as agents of influence (Kragh, Martin and Sebastian Åsberg 2017, 17).

Another case study with focus this time on the Finland showed that there were similar tactics being employed by the Russian government for the purpose of confusing the information
environment within Finland. Author Jessikka Aro, in her article “The Cyberspace War: Propaganda and Trolling as Warfare Tools,” highlights several examples. She states “Aggressive pro-Russia troll campaigns have manipulated the public debate and silenced Citizens” (Aro 2016, 122) and “they created their own falsified narrative of me and my article, and spread lies on fake news sites about me…” (Aro 2016, 123). Jessikka Aro had been at the time an outspoken Finnish journalist that had published anti-Russia articles trying to expose the use of information warfare within her country. She was called names in the Russian press and was targeted by a variety of tactics associated with disinformation operations. At the time of her research and outspoken published articles, she highlighted the fact that ”pro-Russia online disinformation is designed to meet the needs of as many different target audiences as possible. The primary target group for the St Petersburg troll factory seems to be ordinary citizens, but politicians and other public figures are targeted as well” (Aro 2016, 124). An important piece of information to take away from that statement is that regardless of their status in the society, the Finnish populace were the targets for the disinformation. This is yet another example of the Russian government targeting and external population to spread whatever message they deem necessary.

Aro also describes some of the specific themes and messages that were passed via social media trolls with examples that include: Western political leaders depicted as Nazis or fascists, images of corpses and alleged war crimes committed by Ukrainian soldiers, and photos of Ukrainian teenage girls wearing t-shirts with Nazi symbols on them… all edited in Photoshop (Aro 2016, 125). Additionally, she points out that “many fake news sites, such as Sputnik, describe their content as ‘alternative’. In reality this usually means ‘pro-Russian’, ‘conspiracy theoretical’ and ‘anti-Western’. Articles critical of Putin’s regime are not published” (Aro 2016,
Lastly, the author Steven Livingston points out similar concepts to what was already mentioned in the previous two examples, saying “in St. Petersburg, a Russian ‘troll factory’--a facility filled with paid online disinformation artists--pumps out fake information in efforts to obfuscate Russian war crimes in Ukraine and Syria and retaliate against Western investigators” (Livingston 2017, 2). He also highlights the case of Jessikka Aro being targeted by Russian social media trolls.

Overall, there are couple highlights to take away from the Nordic case studies. One, there was a wide variety of tactics utilized within both Sweden and Finland, to include: Targeted media campaigns, social media trolling, forged interviews, and fake news stories. Additionally, the target audience in this effort was the Swedish and Finnish speaking populations of each respective country, and not necessarily the domestic population of Russia. This analysis is the start of the pool of research that has been collected.

**Baltic Nations Case Study**

Moving on to the next area of focus, Pranas Ciziunas compiled a case study that looked at all three Baltic nations as a hotspot for Russian disinformation. He identifies Russian soft power tools and levers that have all been utilized in the Baltics already to include: diplomatic efforts, disinformation campaigns, military threats deployments in the area, economic and energy leverage, the exploitation of ethnic and social differences, and the discrediting of governments via political influence and intelligence services (Ciziunas 2008, 288). While all those factors are in play in the broad spectrum of geopolitics, the article presents some great examples of specific disinformation tactics utilized in the Baltics.

Russian disinformation in the Baltic states takes the form of tactics that are similar to
what was observed in the Nordic countries mentioned above. The Russian government has used “propaganda and disinformation campaigns leveraging Russian and international media, both newspapers and TV are still used to influence public opinion throughout the region and, particularly, in Russia” (Ciziunas 2008, 290). While this hints at the use of these tactics to sway the domestic Russian population, Ciziunas also notes that “…the Kremlin can influence the information provided by many major news media outlets in the former Soviet Union…” (Ciziunas 2008, 290). An example of this was the disinformation campaign used to discredit the expansion of NATO to the borders of the former Soviet Union. The Russian press would purposefully interview and cite individuals who would speak out against NATO and the nations that host forces on the ground near Russia. Additionally, Russian officials and media was argue that NATO threats would encourage extremist groups (in this case in the Baltics) to challenge the current governments.

Other disinformation tactics were also used to try and discredit the current Baltic governments and their supporting parties. In Latvia, for example, the Russian government “used propaganda campaigns against Latvia to make the government look bad” (Ciziunas 2008, 300). Examples of this included media releases and interviews that accused the Latvian government of being fascists, that the laws within Latvia violated the rights of the ethnic Russians living within the country, and that there is a general policy of discrimination against the minority Russians within Latvia.

In all, there were less obvious tactics being utilized in the Baltics, at least based on the case study provided. The main tactics described above included the use of a targeted media campaign and the use of fake interviews to spread a specific message. Additionally, the message has been targeted at the populations that live within the respective Baltic nations, to include the
native speakers and the ethnic Russian minorities of each of those countries. The body of research continues to expand.

**Ukraine Case Study**

The next area of focus is the Eastern portion of Ukraine that saw the rise of separatist forces and the employment of Russian forces under the guise of Ukrainian paramilitaries. Immediately Michael Kofman and his fellow authors identify social media as a major tool used by the Russian government during this conflict. It became one of the important ways in which they were able to message their disinformation, as well as, block messages they did not want to spread. For example, Kofman et al point out that “because the two most popular social-media platforms in Ukraine, VKontakte and Odnoklassniki, were hosted on Russian servers, Russian authorities were able to block pro-Maidan pages…” (Kofman et al. 2017, 50). Additionally, they were able to “…force service providers to share personal information about those who ‘liked’ them” (Kofman et al. 2017, 50). While this tactic doesn’t specifically push a message like those identified in the other case studies, it helps shape the information environment in a positive light for the Russian government. They are able to control more of the information space to then have more of their targeted media efforts available to the general public.

When it comes to the general public in this case, the events of Eastern Ukraine saw something a little different than what the previous case studies have described. In this case, the Russian government was actually for the most part targeting their internal domestic population with their information effort. There were some efforts to target the Ukrainian population with specific messaging, but those efforts fell flat. When it came to the domestic Russian population, however, “the information campaign was most effective on the Russian population, popularizing the mission of the separatists and endowing them with a purpose” (Kofman et al.
In all, there was limited academic analysis available to provide specific tactics and data to this overall compilation of disinformation information. What was pulled from the case study was the use of social media as a platform for targeted media disinformation operations, as well as, the first example of the Russian populace as the targeted audience.

**Crimean Peninsula Case Study**

Next on the list of case studies revolves around the events of the Russian takeover of the Crimean Peninsula. There has been a significant amount of research and analysis done covering these events, and that provided a large amount of data to this content analysis.

To start, Anton Bebler in his case study titled “Crimea and the Russian-Ukrainian Conflict” noticed that immediately after the takeover of Crimea by Russian personnel, there were several actions taken to control the information environment to include the shutdown of Ukrainian television channels, the prevention of Ukrainian printed media from being dispersed around the peninsula, and the kidnapping of fifteen pro-Ukrainian journalists and activists (Bebler 2015, 42). Due to these actions, as well as, a well-coordinated disinformation campaign “the population of Crimea was thus subjected to one-sided information and often outright disinformation by the Russian state-controlled mass media” (Bebler 2015, 42). Bebler describes this disinformation as an “intense propaganda campaign” similar to the efforts conducted by the Soviet Union for the Cold War (Bebler 2015, 42). Additionally, there were reports of targeted media themes to paint the Ukrainian government as fascists and neo-Nazis, spread fake news stories and messages about the discrimination and “genocide” of the ethnic Russian and Russian speaking populations of the Crimean Peninsula, as well as, the harassment of Crimean Tartars by the forces on the ground.
In a similar vein, Michael Kofman and his fellow authors described a similar situation during the annexation of the Crimean Peninsula. In their study, the identified examples of Russian disinformation tactics and specific messaging themes pushed by the Russian government that preceded, accompanied, and followed the annexation of the Crimean Peninsula. They point out that “[the disinformation campaign’s] primary audience was the Russian public at home, with Crimean residents as a secondary consideration (Kofman et al. 2017, 12). The Russian television messaging focused more on influencing the domestic audience than it did trying to influence the Ukrainian audience, or even the Western audience.

Interestingly, Kofman and his associates make the statement that “Russia did not create special agencies, tools, or media to engage Ukrainians in Crimea. Information operations aimed at Ukrainian citizens were essentially a by-product of Russia’s information campaign to manage its own domestic opinion” (Kofman et al. 2017, 29).

On top of those pieces of vital information, Kofman and his fellow authors also dissected the types of tactics and tools utilized by Russian in their disinformation campaign that played throughout the Crimean conflict. For example, Russian controlled media channels in Russia, the West, and Ukraine used a combination of news reports (both real and fake), talk shows with special guests chosen for a purpose, and documentaries that carried the theme the government was trying to portray. Additionally, Russian agents used a combination of Russian, Ukrainian, and Western websites as platforms for sharing news stories and propaganda, with social media acting as a major vehicle to pass the information, printed press in a similar vein, as well as, leaflets and billboards to cover all their bases. All of this information, in all its different forms, were directed at the internal Russian population in order to keep everyone informed in the way that the Russian government wanted them to be. What the message was at the time was
what people were going to see.

As to the special guest speakers that Russian employed on television channels, repeated on news stories, and blasted across social media, they sought out specific individuals and personalities to help progress their message. That included the President Vladimir Putin, Sergei Lavrov, and other Russian politicians as the figure heads pushing the message. Additionally, they used clips from Ukrainian politicians and experts to make sure that their message was portrayed from the Ukrainian perspective regardless of the context of those clips. The Russian government and media apparatus also used pro-Russian organizations and political parties in Ukraine, Western politicians and experts from Europe and the United States, Local protest leaders, regular citizens and “professional” protest participants, and celebrities and intelligentsia (Kofman et al. 2017, 82).

Throughout the conflict, “the Russian media always maintained some coverage on events in Crimea for its own domestic public, but this intensified as the clashes between the pro-government forces and the protesters in Kyiv grew more violent” (Kofman et al. 2017, 12). Again, this case study conducted a thorough analysis of the data and was able to identify five major components that were being messaged throughout the conflict. As expected, social media remained one of the major platforms for which the disinformation media was disseminated. The five major themes were: massive and long-lasting impact (repeat the same themes over and over again), desired information (manipulate messages to play upon the fears of ethnic Russians in Ukraine), emotional agitation (use themes that will make ethnic Russians in Ukraine act out of irrational anger), clarity (present the Ukrainian conflict in simple terms of good and evil), supposed obviousness (match propaganda messages with widely held Russian myths and legends) (Kofman et al. 2017, 28).
In conclusion, there was a lot to take away from the analysis of the Crimean conflict back in 2014. First of all, the targeted population, like that of the events in Eastern Ukraine, was the internal domestic population of Russia, and secondarily the people of Crimea, Ukraine, and the West. Additionally, there were a wide variety of tactics utilized during the conflict to include: the control of media dissemination platforms to control the information environment, the use of targeted media campaigns to send specific messages, the use of social media as a major platform to disseminate information, the employment of actors and agents to lend credibility to the message being dispersed, and tactics as simple as leaflets and billboards.

**General Disinformation Operations**

This next category is not based around a specific region, or nation, but instead encompasses the case studies that have been conducted as a general look at Russian disinformation tactics and campaigns. This portion of the content analysis will not necessarily add to the nation specific look at the data during the QCA portion of the analysis, but provides an additional insight into the types of tactics that have been used by the Russian disinformation apparatus.

According to authors Christopher Paul and Miriam Matthews, the “[Russian government’s disinformation] tools and channels now include the Internet, social media, and the evolving landscape of professional and amateur journalism and media outlets” (Paul and Matthews, 2016, 1). They also describe the disinformation operations as rapid, continuous, and repetitive with little to no focus of consistency or regard for truth. In all, the individual tactics utilized by the Russian government are produced and dispersed in large volumes in order to ensure that a large number of channels and consumers receive the information, and that the information makes it to the top headlines and pages of websites. Paul and Matthews point out
“this propaganda includes text, video, audio, and still imagery propagated via the Internet, social media, satellite television, and traditional radio and television broadcasting (Paul and Matthews, 2016, 2). These medias span almost the entire spectrum of available resources that any audience might utilize to receive their news information. This is of course helped along by the use of paid internet trolls that focus their effort to online chat room, forums, and comments sections of Russian produced and non-Russian produced internet articles. Based on the research the authors were able to complete, it was discovered that “the trolls are on duty 24 hours a day, in 12-hour shifts, and each has a daily quota of 135 posted comments of at least 200 characters (Paul and Matthews, 2016, 2).

On a different note, RT acts as one of the main media organizations peddling the disinformation tactics through to a large audience. Paul and Matthews point out that RT maintain :a budget of more than $300 million per year, it broadcasts in English, French, German, Spanish, Russian, and several Eastern European languages” (Paul and Matthews, 2016, 2). Also “in addition to acknowledged Russian sources like RT, there are dozens of proxy news sites presenting Russian propaganda, but with their affiliation with Russia disguised or downplayed (Paul and Matthews, 2016, 2).

Another consideration for these specific types of tactics used in Russian disinformation is that there is usually a significant amount of work done to create news that seems as legitimate as possible, even if the entirety of the story and source is made up. According to Paul and Matthews “Russian news channels, such as RT and Sputnik News, are more like a blend of infotainment and disinformation than fact-checked journalism, though their formats intentionally take the appearance of proper news programs” (Paul and Matthews, 2016, 5).

What that means, is that a significant amount of time and money is spent by these organizations
to fabricate as legitimate news articles as possible. A great example provided by the authors was that of RT quoting a well-known blogger and critic of Syria’s Assad regime about the chemical weapons attack in Syria. They use his analysis of the videos being posted online and push his version of the story as the ground truth; leaving no question that Assad was behind the attack and no one else.

Looking at some other examples, author Leon Aron provides some context that ties this type of warfare back to the overarching framework of New War Theory. He states ”It is here that what is known as the ‘weaponization of information’ occurs: news and analysis as a means of provoking strong negative emotions, potentially leading to hatred, incitement and, ultimately, the justification of violence” (Aron 2016, 2). Information is used to try and win the hearts and minds of certain groups, or at the very least affect the way certain peoples and groups view the world around them.

Author Kenneth Weinstein provides a similar analysis to that of Paul and Matthews stating “well-funded state propaganda outlets designed to have the patina of impartial media outlets include Russia’s RT, Sputnik, Ruptly, Rossiya Segnodnya, and other secondary platforms, which according to State Department estimates spends over $1.4 billion annually on propaganda. (Weinstein 2017, 4). This information is also demonstrated in Heather Conley’s article, where she says “RT purports to reach over 700 million people and has an annual budget comparable in size to the BBC's World News Service (Conley 20, 3). According to her, the use of fake news, messaging across multiple media platforms, and the use of similar tactics described by Paul and Matthews are all a part of the overall game plan for Russian disinformation operations.

Overall, that leaves this research with a solidified amount of data and examples to piece
together for the overall summary. The general look at disinformation has provided several more cases that describe the use of a targeted media campaign, the use of social media as a platform, and the use of Russian backed and funded news organizations like RT and Sputnik. It also shows a lack of regard for truth demonstrated by the use of fake news, fake interviews, and the spooning of information that represents the answer Russia wants messaged out to the world and its own people, not necessarily what is true.

**Syria Case Study**

While Syria, as the last category, does not fit the mold created in the introduction and the rest of the paper, it is worth examining tactics used outside of eastern Europe to act as a pseudo control case study. Additionally, since Syria does not fit in the mold, the information gained here was not used in the QCA conducted later in the study.

According to the author Steven Livingston, one of the major approaches used by the disinformation actors of Russia is to push a “tsunami of confusing, contradictory disinformation” (Livingston 2017, 3). The strategy is less about introducing specific stories, or fake news, and more about introducing enough information into the media world to add confusion across the board. For example, Western and Middle Eastern news agencies have published several stories, graphs, and images depicted the use of chemical weapons, barrel bombs, and air strikes against hospitals by the Syrian and Russian governments. However, the Russians have continued to counter the messaging with news stories that either directly contradict what’s being reported, or at the very least add enough confusion about what the truth to create doubt. This was done through the use of fake news articles, staged interviews, and discrediting reports about the original agencies and organizations that published the stories to begin with. Additionally, in specific example, “a Russian Ministry of Defense official presented
satellite imagery he said confirmed that [a] hospital had not been attacked as the news media claimed. He presented side-by-side satellite imagery to claim that reports of airstrikes on a hospital were mere fakes” (Livingston 2017, 3). However, this was then countered by the Western press in order to validate the original story as it was presented.

In all, while this specific case study does not add data points and analysis used later in the QCA, it does bring something important to light. Similar tactics are being used across the board by the Russian disinformation machine, and those include fake interviews, fake news stories, and social media as a platform to push information. Additionally, those tactics are directed, in this case, at anybody who is looking into the stories in Syria. In this paper, that means both the domestic and external populations with respect to Russia.

**Commonalities**

In summary, there are a lot of similarities between the different case studies examined for this paper. In order to make sense of them, this section is going to look at three main topics by case study: targeted audience, common tactics, and common themes.

It is important to remember this information in the context of New War Theory as well. As a review, Mary Kaldor describes New War Theory as the developing way modern wars are being fought and that those wars are fought more over identity and in the name of groups than the traditional use of the military as a political tool to gain territory, resources, or standing in the world. Additionally, new wars depend less on military violence to capture territory, but instead “battles are rare and territory is captured through political means, through control of the population” (Kaldor 2013, 2). It is in this context that Russian seeks to make it moves around the world, and specifically on their doorstep in eastern Europe. It is through this lens that the following discussion on themes and tactics should make sense because it is exactly this type of
warfare that is being conducted by the Russians.

To start, one of the difficult things to pull out of the case studies, was who exactly was the target audience. In some cases, like that of Sweden, it was a little easier to determine due to the fact that the case study focused on the use of the Swedish language channel of Sputnik for their research. It’s not a stretch to say that the Swedish population was the target audience in that specific case. Additionally, Russian government owned media outlets have created channels in many other languages, to include some of the other examples examined like Finland and the Baltic nations. There have also been English language channels created, like in the cases for Syria, that help disseminate information to as large an external audience as possible. The cases of Ukraine and Crimea, however, saw a much different focus by the Russian government. A majority of reporting done during those conflicts was done in Russian and was meant to sway the domestic population of Russia. It is worth pointing out that there was an unsuccessful attempt at swaying the Ukrainian audience by silencing radio and news stations. It is through those case studies that one can see that the Russian disinformation campaigns are not targeted against one specific group, but are used across the board to drive home Russian government objectives. When things in Syria and Ukraine were looking bleak based on Western reporting, it would make sense that disinformation tactics are used to sway the domestic population back. In contrast, when opinion of Russian motives and ways are already low in certain areas, it makes sense that those areas be targeted differently. In the cases this paper examined, each country within the Eastern half of Europe was targeted differently and in their own national language.

It is important to remember that this is all accomplished through the lens of New War Theory, and at this point the picture should be relatively clear. Regardless of the objectives that the Russian government was trying to achieve, they are focusing their efforts on winning over
specific groups and targeting specific people. It is less about gaining territory specifically, and more about who the viewer of a fake news article, or fake interview is going to be. This falls right in line with what Mary Kaldor argues regarding New War Theory in that modern conflicts are fought over identities and for groups of people, not necessarily nation states. Additionally, military advances and seized territory are less important compared to winning the hearts and minds of individuals and groups.

That leads into the next section of this analysis: the most common tactics identified throughout the case studies. In all five areas that were examined (Sweden, the Baltics, Ukraine, Crimea, and Syria) the use of a targeted media campaign was one of the primary tactics used. An issue would arise, like the shoot down of MH47 or bombing of hospitals, and a flurry of media activity would ensue. The main objective of this tactic was to introduce as much confusing and potentially contradictory information into the minds of viewers as possible in order to either misrepresent what was happening on the ground, or cause enough chaos that nothing would every happen internationally. As previously mention, depending of the event, the audience could be people on the ground, the external populations that care of about Russian activity, or the domestic population of Russia. Another common tactic used was social media trolling. In the case of Sweden, Finland, and identified in the general studies of Russian disinformation, there were several instances of Russian trolls and/or bots on social media sites that would push certain themes, post so many times that the same articles were at the top of people’s news feeds, or overwhelm anti-Russian sites and reporters. Next, there was a consistent use of fake news articles, false information, and fake interviews that were pushed either via media outlets, or through the use of social media trolls. These tactics were identified nearly across the board in Sweden, the Baltics, Crimea, Syria, and describing the general us of
disinformation by the Russian government. In many cases, the Russian media outlets would find someone who was extremely biased towards an event on the ground to interview, or would just fabricate the interview and story all together. Again, these tactics were used to target a specific population and to push specific Russian objectives. Lastly, social media has been widely used throughout each of the cases as one of the primary tools for disseminating disinformation. In Ukraine, Crimea, Syria, and in general, the Russian disinformation machine has pushed tons of information, to include the fake interviews and articles, on social media as a fast, easy method of reaching people globally. They have used the speed and interconnectivity that social media brings to the world as an information weapon against whoever they deem necessary.

In the context of New War Theory, these tactics fit right into the mold. As previously mentioned, the idea behind New War Theory is that people and groups are the most important commodity being fought over, and that the fighting is conducted in the name of identity. Additionally, it is not necessary for military action on the ground to be the method at which people and territory are won, but instead things like information operations can be more effective.

Lastly, there were several common themes identified throughout the cases studies and across all regions examined. Several of these were pro-Russian themes, for example, some articles and social media posts were pushing for a positive image of Russia, or indirectly drove for international sympathy for Russia. However, some of the themes were starkly anti-western in their nature. They pushed themes like there is a crisis in the West, NATO aggression against Russia, malicious activity by the West, and overall policy failure in Western natures. Additionally, several stories took advantage of small riffs between Western allies to highlight
the lack of cohesion and to drive home the idea that Western alliances were falling apart. All of this was done in the name of New War Theory in that it is meant to sway the opinions and beliefs of people all over the war. Different tactics and stories were pushed against different people and nations, but their goal was to sway people towards Russia or away from their tightly held western biases.

In all, there were a series of common tactics and themes identified within each case study and through the content analysis. It is from this information that the data used for the QCA was identified and selected. These ideas and concepts are important to remember and identify going forward, because as Russia gains a stronger foothold on the world stage, one can expect to see a lot more of this happening. By identifying and labeling disinformation operations by the Russian government, it allows for further analysis and the development of counter tactics down the road.

**QCA Structure**

In addition to a content analysis that identified common trends and tactics throughout multiple different case studies, this study also looked at some of the casual factors that present the right environment for Russian disinformation operations.

The first phase of the QCA was to identify relevant cases and causal conditions. What that meant for this paper was that there had to be specific case studies identified and analyzed and those case studies had to be binned into one of two categories. First, disinformation tactics were used against the domestic Russian population in order to sway their view, or understanding of a situation. Second, disinformation tactics were used to target an external population to try and deceive, or misinform them. What that means is that the outcome for the QCA was the targeting of external populations, so the positive cases reflected that and the
negative cases did not.

Based on the research that was completed, there were five identified positive cases: Finland, Sweden, Lithuania, Latvia, and Estonia. On the other hand, there were only two negative cases identified: Eastern Ukraine and Crimea. Together, these cases represent the relevant cases for the analysis, and they constitute the overall sample population with a sample size of only eight.

Next, based on the relevant cases and outcome, as well as, relevant knowledge and theory from the remaining sources, the next step was to identify potential casual conditions for the cases mentioned above. This study identified seven casual factors to analyze that included: 1) if the country in question was previously a part of the Soviet Union 2) if the target nation had a segment of their population that spoke Russian/was an ethnic Russian 3) the target country was pursuing policies that leaned towards the West 4) whether or not the country was a member of NATO 5) if the target country physically bordered Russia 6) if Russian media broadcasts were available in the country in question, and 7) if the Russian media apparatus had produced a target nation platform in their indigenous language.

These seven variables were chosen for specific reasons, and were meant to be the most streamlined, or consolidated, variables available to help explain the context of Russian disinformation in Europe. Discovered in the content analysis were themes that included anti-west narratives, anti-NATO narratives, narratives that were geared towards the ethnic Russian population of neighboring countries, and a variety of tactics that were used to push those themes. Therefore, the focus of the variable selection was meant to highlight those very things. Membership in NATO and policies that were democratic in nature, or leaned towards the west (e.g. the E.U. and the U.S.), were covered by their own individual variables. Additionally, if
there was a Russian speaking population within the targeted country, that would be important if the narrative was geared in their direction. The remaining variables cover the types of tactics utilized (i.e. the creation of target nation language media stations) and the history of the area and the impacts of the fall of the Soviet Union (e.g. former Soviet territory and border countries). With those variables chosen and the cases set for analysis, the following sections describe the computations done to discover patterns and answers within the data.

**Computations**

The first analytic look at the data was conducted through the use of a manually created truth table. The truth table is an example of a QCA and provides the analyst an ability to look at every possible outcome of events based on the chosen variables for the analysis. In order to complete the truth table the positive and negative cases had to be identified based on the chosen outcome. The outcome, as mentioned above, was that an external audience was targeted as part of the Russian disinformation operations. A positive case was tallied if the variables were matched the truths listed in Table 1, and was not tallied if the variables did not match the particular logical case. The same was also true for the negative cases. Table 1 shows all the positive and negative cases that were used for the QCA and are based on the analysis done in the content analysis above.

**Table 1. All positive and Negative Cases with Truth Values.**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Finland</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Lithuania</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Latvia</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Estonia</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Ukraine</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Crimea</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
The truth table depicted in Table 2 is the result of some cleaning up from the fully developed truth table. The original truth table looked at every possible case that could logically exist given all seven variables and was given a weight based on the number of positive and negative cases present. Any consistency values that resulted in a one or a zero resulted in a perfectly consistent case, and all cases with a value between zero and one were considered inconsistent. Cases with a .5 in their consistency value were considered perfectly inconsistent. The resulting values in figure two show all the possible logical cases that had positive and consistent outcomes, therefore represent the most likely variables combinations that could provide the context for Russian disinformation operations. In other words, these combination of variables represent environments in which one could expect Russia to conduct some form of disinformation operation. Interestingly, the common variable among all the positive and logically consistent possibilities was that the country was a NATO member.

**Table 2. All Positive and Logically Consistent Cases.**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>22</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>34</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>35</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>41</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>42</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>48</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>49</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>51</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>53</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>57</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>58</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>59</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
<tr>
<td>62</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1.000</td>
</tr>
</tbody>
</table>

**Totals:** 6 10 11 18 7 8 0
The next analysis completed was completed in a similar fashion to the manually created truth table. However, this time was completed using a Crisp-Set Analysis software that provided a little more analysis of the data than simply looking at all positive and logically consistent possibilities as a result. The Crisp-Set Analysis is a form of QCA that uses a truth table, Boolean logic, and comparative logic to minimize the cases that do not fit the provided combination of variables and to eliminate cases that provide similar results. In other words it uses logic to reduce complexity and provide a simplified analysis that can help describe a situation. It is similar in outcome to the manual truth table method used above, however, the outcomes look slightly different. By conducting a Standard Analysis of the data, the software provided three types of results. According to one of the user’s guides for the Crisp-Set QCA (csQCA):

fsQCA [and csQCA] presents three solutions to each truth table analysis: (1) a “complex” solution that avoids using any counterfactual cases (rows without cases—“remainders”); (2) a “parsimonious” solution, which permits the use of any remainder that will yield simpler (or fewer) recipes; and (3) an “intermediate” solution, which uses only the remainders that survive counterfactual analysis based on theoretical and substantive knowledge (which is input by the user)” (Ragin 2008, 13).

A key thing to mention here is that this definition is used in relation to a Fuzzy-Set QCA, and not a csQCA. The main difference between the two types of techniques crisp-set QCA uses only 1 and 0 as the only answers possible, whereas, fuzzy uses values from 1 to 0. The limitation in using a crisp-set QCA is that there is little variation introduced into the possibilities, therefore, a condition is either met or not. There are inherent limitations in describing complex geopolitical
situations with that method, but it provides an easier analysis with many variables. In either case, however, the results are still displayed using the same three types of solutions described above.

Figure 1 listed below is the complex solution that was the output of the software using the same positive cases, negative cases, and variables that were used for the manual truth table. The results show the three logical cases that present logically consistent scenarios listed with their values in terms of raw coverage and unique coverage. Raw coverage means represents the extent to which each combination of variables can represent the outcome, and unique coverage means the proportion of cases that can be explained exclusively by the combination of variables. In this case the top complex result shows that a nation that is a former Soviet territory, has a Russian speaking population, has policies that lean towards the West, is a NATO member, borders Russia, and has access to Russian media broadcasts within their media architecture is the most likely to be a target of Russian disinformation operations. Again, as the result of a complex solution, this means none of the solutions were simplified or eliminated and provides the most complex possibilities as a solution.

<p>| --- COMPLEX SOLUTION --- |</p>
<table>
<thead>
<tr>
<th>Raw coverage</th>
<th>Unique coverage</th>
<th>Consistency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Result 1</strong></td>
<td>FormerSovietTerritory?*RussianSpeakingPopulation?*Policiesleantowardsthewest?*NATOMember?*BordersRussia?*Russianmediabroadcastsavailable?</td>
<td>0.6</td>
</tr>
<tr>
<td><strong>Result 2</strong></td>
<td>~FormerSovietTerritory?~RussianSpeakingPopulation?*Policiesleantowardsthewest?~NATOMember?~BordersRussia?~Russianmediabroadcastsavailable?*Targetnationlanguagebroadcastsavailable?</td>
<td>0.2</td>
</tr>
<tr>
<td><strong>Result 3</strong></td>
<td>~FormerSovietTerritory?~RussianSpeakingPopulation?~Policiesleantowardsthewest?~NATOMember?~BordersRussia?~Russianmediabroadcastsavailable?*Targetnationlanguagebroadcastsavailable?</td>
<td>0.6</td>
</tr>
</tbody>
</table>
Figure 1. Complex Solution to the csQCA.

Next, looking at the parsimonious solution to the csQCA, the results in Figure 4 show that there are two logically consistent possibilities for the positive cases, negative cases, and variables used in the analysis. In this case, the top result was that a NATO member nation would be the most likely candidate for the Russian disinformation apparatus. Again, as a parsimonious output, this means the solutions have been reduced to the smallest number of conditions possible. Therefore, it represents the simplest solution possible.

<p>| --- PARSIMONIOUS SOLUTION --- |</p>
<table>
<thead>
<tr>
<th>Raw coverage</th>
<th>Unique coverage</th>
<th>Consistency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result 1</td>
<td>NATOMember?</td>
<td></td>
</tr>
<tr>
<td>0.6</td>
<td>0.6</td>
<td>1</td>
</tr>
<tr>
<td>Result 2</td>
<td>~Russianmediabroadcastsavailable?</td>
<td></td>
</tr>
<tr>
<td>0.4</td>
<td>0.4</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 2. Parsimonious Solution to the csQCA.

Lastly, the remaining results listed in Figure 5 show the solutions to the intermediate analysis. Based on all the positive cases, negative cases, and variables used in the analysis the top result showed that a nation that was a former Soviet territory, had a Russian speaking population, had policies that leaned towards the West, was a NATO member, is a country that borders Russia, and has access to Russian media broadcasts as part of their media collective was the most likely candidate for Russian disinformation operations. This result presents the same solution that was provided as the output to the complex analysis. Again, as an intermediate
solution the result was computed by introducing some additional positive and negative factors to reduce complexity, but not completely eliminate solutions down to their simplest form. Therefore, intermediate solutions are usually regarded as the best solution.

--- INTERMEDIATE SOLUTION ---

<table>
<thead>
<tr>
<th>Raw coverage</th>
<th>Unique coverage</th>
<th>Consistency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policiesleansowardsthewest?<em>-NATOMember?</em>-Russian mediabroadcassetsavailable?*Targetnationlanguagebroadcastsavailable?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.2</td>
<td>0.2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>-NATOMember?<em>BordersRussia?</em>-Russianmediabroadcassetsavailable?*Targetnationlanguagebroadcastsavailable?</td>
</tr>
<tr>
<td>0.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FormerSovietTerritory?*RussianSpeakingPopulation?*Policiesleansowardsthewest?*NATOMember?*BordersRussia?*Russianmediabroadcassetsavailable?</td>
</tr>
<tr>
<td>0.6</td>
</tr>
</tbody>
</table>

**Figure 3. Intermediate Solution to the csQCA.**

**Analysis**

Overall, the analysis has shown three main points that are worth recapping here in a final analysis summary. First, the messaging and themes from Russian disinformation, as well as, the result from the manual truth table analysis and the csQCA parsimonious analysis have shown that countries that are members of NATO are at risk for Russian disinformation operations. Additionally, part of the results of the complex solution and intermediate solution for the csQCA contain results with the NATO member variable. Secondly, the complex results of the csQCA show that nations that are a former Soviet territory, have a Russian speaking population, have policies that lean towards the West, are a NATO member, border Russia, and have access to Russian media broadcasts within their media architecture are the most likely to be a target of...
Russian disinformation operations. Lastly, the results of the intermediate csQCA analysis show that nations that fit the same description listed for the complex solution are all at risk to Russian disinformation operations.

To the first point, this should be of no surprise to anyone reading this paper, for anyone who has studied Russian foreign policy for a brief period, or for anyone who lived through the height of the Cold War. However, what this research provides are the specific examples and computed results that show that this remains a constant in Russian foreign policy. More specifically, Russian disinformation operations tend to target populations that exist within current NATO member nations. Ultimately, what this means is that one can look to places in the rest of Europe, places like Poland for example, that are close to the periphery of Russia and are a member of NATO, as a place that could potentially be targeted by Russian disinformation operations as the growth of Russian influence and operations continues in a positive slope. Additionally, one can expect to see at the very least the types of tactics identified in the content analysis and, depending on the objectives, could expect any NATO member’s populace to be targeted in a disinformation campaign.

The second point, the results of the complex csQCA, show an interesting combination of variables that could provide the necessary recipe to understand the most likely locations to expect Russian disinformation operations, or at the very least the bulk of the Russian focus. While this combination of variables does not lead to many other future scenarios, it can still spell out the environment in which Russia is most likely to operate. Potentially the variables are prioritized by Russia in a way that was not factored in for this analysis, which could mean that other nations that fall close to the combination of variables depicted in the complex analysis might be susceptible to future disinformation campaigns. This might be particularly true for
nations that have a Russian speaking population, are on the border or close to the border of Russia, and are seeking NATO membership, like Georgia, Macedonia, and Bosnia and Herzegovina.

Lastly, similar to the complex results of the csQCA, the intermediate results show the most likely environment in which Russian disinformation operations could be expected. The nations that fall in line with the given variables are the most likely to fall victim to Russian disinformation, and like mentioned above, nations applying for NATO membership might be excellent candidates as targets, especially those that closely mirror said variables.

Overall, the two-pronged approach to this research has laid out the types of tactics used by the Russians in their disinformation operations, it has identified case studies where disinformation tactics were utilized, the results and themes produced through those tactics, and the variables that best describe nations and people that are likely to be targeted by Russian disinformation.
CHAPTER FIVE

CONCLUSION

In conclusion, this research paper was designed to identify specific patterns, tactics, and messaging used by the Russian government and its state-run media in order to conduct disinformation campaigns against targeted audiences. Several case studies have been completed that look at tactics used, the end state of the Russian disinformation, or at the very least the potential outcomes; however, no study had combined these case studies to examine for patterns and to compile those results into a single source document with references. Additionally, this study looked at the potential variables that could describe the environment in which Russia might attempt disinformation operations using a QCA to analyze the case studies that were studied in the content analysis.

The content analysis provided a more in depth look at the types of tactics used by Russian disinformation operatives, and included targeted media campaigns, social media trolls, fake news, and fake interviews. Those tactics were used against different audiences, but were common throughout. Depending on the message being sent, or the specific objective of the disinformation, the audiences were either external to Russia and represented a group they were trying to sway with confusion, or were the domestic population of Russia that they tried to sway to side with the government. To reiterate, one of the main limitations of this study was that the content analysis relied on peer-reviewed, academic case studies that provided and in depth analysis of specific instances of Russian disinformation operations. Any bias that was a result of those studies being done, and the quality of the research completed within those studies also transferred to this study. Additionally, there were only a limited number of in depth case studies available, but this study looked at examples from several different geographic areas.
Additionally, the QCA that was used was meant to identify potential environmental conditions in which one might expect to see Russian disinformation operations, but was also limited by the number of cases and the case studies that were analyzed for the content analysis.

Based on all that research, there were several key highlights out of this study. The tactics identified were common throughout most of the case studies examined, therefore should be expected in the event of continuing or future disinformation operations by the Russians. Several QCA results identified the common environmental variables that show the conditions in which one could expect to see Russia trying to influence the people of that area. There were no surprising answers based on the analysis, such as NATO membership being one of the main variables identified for targeting, but this study backs up that idea with content and analysis.

Moving forward what this study has done is provide a baseline analysis for the environment and types of tactics one would expect to see Russian disinformation operations. This will allow for several things. First, further analysis of the cases study areas to identify other types of tactics used, specific populations that are at risk, and a more detailed look at the tactics that have been used (e.g. the Swedish case study). Second, it provides grounds for which one could start examining the media and social media environment in vulnerable countries, such as Poland or Georgia to see if disinformation tactics are being used there and to what end. Lastly, it can be used to help develop counters tactics and contrasting information operations to fight back against the Russian use of disinformation. This is probably the most important next step that should come out of this study, as it will provide the West the ability to push back against Russia in the information realm. As Francine Jaomiasa points out “we have a deeply fracture media and information environment where the first victim is the truth” (Jaomiasa 2016, 43).
References


