Fall 2018

The evolution of computational propaganda: Trends, threats, and implications now and in the future

Holly Schnader

The Evolution of Computational Propaganda: Trends, Threats, and Implications Now and in the Future

An Honors College Project Presented to

the Faculty of the Undergraduate

College of Integrated Science and Engineering

James Madison University

by Holly Nicole Schnader

December 2018

Accepted by the faculty of the College of Integrated Science and Engineering, James Madison University, in partial fulfillment of the requirements for the Honors College.

FACULTY COMMITTEE:

Project Advisor: Timothy Walton, Ph.D.
Associate Professor, Intelligence Analysis

Reader: Edna Reid, Ph.D.
Facilitator, Intelligence Analysis

Reader: Kathleen Moore, Ph.D.
Assistant Professor, Intelligence Analysis

Reader: ,
,

HONORS COLLEGE APPROVAL:

Bradley R. Newcomer, Ph.D.,
Dean, Honors College

PUBLIC PRESENTATION

This work is accepted for presentation, in part or in full, at Intelligence Analysis Targeting Speaker Event on January 2018.

James Madison University

The Evolution of Computational Propaganda

Trends, Threats, and Implications Now and in the Future

Holly Nicole Schnader

Intelligence Analysis, College of Integrated Science and Engineering

Project Advisor	Dr. Timothy Walton, Intelligence Analysis Associate Professor
Reader	Dr. Kathleen Moore, Intelligence Analysis Assistant Professor
Reader	Dr. Edna Reid, Intelligence Analysis Facilitator

Dedication

This work is dedicated to the Intelligence Analysis program at James Madison University for providing me with a multitude of different opportunities, for challenging me, and for sparking my interest in the cyber field which has led to me finding my future career path. This work is also dedicated to my classmates, friends, and family, for supporting me in all my endeavors and encouraging me to pursue my interests and dreams.

Preface

Computational propaganda is becoming an increasingly important, complex, and critical topic of discussion. Especially since the activities related to the 2016 United States presidential election, this newer form of psychological and cyber warfare has grown in interest. However, with increased discussion in the world, also comes confusion and misunderstanding about what computational propaganda is, how it came to be what it is today, and how it will likely evolve in the future.

Unlike conventional warfare and the tactics used, which have a longstanding history, cyberwarfare and its techniques, such as computational propaganda, are comparatively new. Thus, the conventional wisdom on this topic is continuously developing and changing as people gain a stronger understanding of the field. So, it can often be difficult to find up to date sources and information to expand upon. However, the use of propaganda and influence tactics is not new and has been used for centuries in order to accomplish certain goals.

In this paper, I plan to analyze and identify a likely future outcome related to computational propaganda. I will comprehensively discuss the likely future outcome, the authoritative assessment, based on causal forces identified early in the analysis. I will also identify an alternative and exploratory outcome using the futures generation technique. By identifying a potential future outcome, the indicators that can be identified prior to reaching that scenario, implications, and mitigation strategies, a plan of action can be developed to lessen the impact of crucial scenarios. I hope to challenge conventional wisdom through scenario generation and provide a value added to the field that can help organizations better prepare for the effects that computational propaganda may have in the future.

As noted earlier, the information on this topic is ever-changing, just like the technology itself. This continuous evolution truly sparked my interest because of my love for learning. Constantly having to learn and adapt new ways of thinking can be challenging, but it is extremely rewarding. I want to learn as much as I can about the field, share what I have learned, and then learn something new about it each day, encouraging others to do the same.

Acknowledgements

The Intelligence Analysis capstone sequence, as well as this Honors capstone project, has been an extremely rewarding experience. Using the information that I collected for my Intelligence Analysis capstone, I was able to broaden my topic to look at and conduct more research on cyber propaganda around the world. Thus, those individuals involved in both capstone projects have been integral to my accomplishments.

First, I would like to express my sincere appreciation for the time that professors, experts in the field, students, and more have invested in my learning and in the success of this project. I want to first thank the advisor for both of my capstone projects, Dr. Timothy Walton. Without your guidance and encouragement, this project and my Intelligence Analysis major capstone would not have been possible.

I also want to thank the readers for my project. First, Dr. Edna Reid, your experience in the cyber intelligence field and your enthusiasm in teaching is what originally sparked my interest in pursuing more projects and a future career in cyber intelligence. Also, to Dr. Kathleen Moore, your knowledge and experience in a number of different fields is inspiring.

I also want to thank all of the faculty, staff, and students in the Honors College that have continued to encourage me over the past four years. This encouragement to stay involved and stay engaged in a higher thinking has inspired me to challenge myself and step outside of my comfort zone.

Finally, I want to acknowledge James Madison University's College of Integrated Science and Engineering for the countless opportunities I have been provided and the support I have received to participate in them.

Abstract

Computational propaganda involves the use of selected narratives, social networks, and complex algorithms in order to develop and conduct influence operations (Woolley and Howard, 2017). In recent years the use of computational propaganda as an arm of cyberwarfare has increased in frequency. I aim to explore this topic to further understand the underlying forces behind the implementation of this tactic and then conduct a futures analysis to best determine how this topic will change over time. Additionally, I hope to gain insights on the implications of the current and potential future trends that computational propaganda has.

My preliminary assessment shows that developments in technology, as well as a desire for improved narrative development will continue to lead to a more personalized narrative. This improved narrative will be more effective at influencing individuals and will ultimately support an organizations' strategic goals.

One aspect of this analysis is to gain knowledge on the evolution of the cyber domain, including electronic propaganda. Another is to better understand the complexity between the pairing of psychological operations with the technical side of this topic, as well as the past effects that cyber propaganda campaigns have had. Through this research, I hope to gain a stronger understanding of the future of computational propaganda and how those in intelligence analysis positions can best discern information that is collected.

The overall goal of this research is to better understand this facet of the cyber domain. As traditional, boots on the ground, warfare techniques become less effective and more costly, alternative methods of warfare will continue to be developed and conducted. Computational propaganda is one of the branches of the cyber domain, falling under information warfare. I aim to identify an authoritative assessment on the plausible future of computational propaganda, as well as identify overall trends, in order to ensure resources are allocated to improving the defensive operations that prove to be adversarial to the United States and allies to the United States.

During data collection, I used academic and credible news sources, think tanks, government reports, as well as reports by credible organizations conducting research on the topic. I also used graphics and diagrams to better understand the technical process that is involved. Additionally, I used the information collected in a previous report that I completed on a "Futures Analysis of Russian Cyber Influence in the United State Political System." I was able to gain a lot of insight from this paper especially because my team and I worked with a sponsor for the project that provided extremely valuable information regarding influence campaigns and echo chambers.

Table of Contents

List of Figures

Executive Summary

Worldwide cyber propaganda activities are likely to become increasingly effective and successful as efforts begin to focus on gaining holistic information and targeting individuals, in order to maintain and strengthen influence campaigns and undermine democratic values. This conclusion is based on an examination of the current trends and dynamics present both technically and politically, the history of cyber influence techniques, and an understanding of adversarial capabilities. The potential future outlined above is plausible given the above factors. Given the appeal and potential benefit for gathering comprehensive data on individuals, entities will likely continue to push for this data collection to better construct influence campaigns.

The collection of information on individuals from social media platforms to devices involved in the Internet of Things (IoT) has become a rapidly growing business. This data is often collected to market convenience for users. From informing an individual about what items are almost gone in their fridge, to showing them items on Facebook ads that they would most likely want to purchase, algorithms and smart devices are being used to collect data and provide conveniences to the user.

Efforts, such as propaganda, have continued to prove successful for many years. State and non-state actors use influence campaigns in order to shape the minds of foreign populations and sometimes their own domestic citizens. These campaigns are unique to users and often contain a narrative that is pleasing to the user, while also attempting to shift their view.

The use of media, including social media in the everyday life of many individuals who are in developed countries, as well as those who are in developing countries, has continued to increase. The interaction with these social networks often leads to users being presented with information from users and pages that they like/follow and sponsored information coming from businesses and organizations. These platforms are most popular for public manipulation because they are low cost and enable organizations to spread information quickly to a lot of users. This enables organizations to achieve many of their strategic goals, like creating dissent among a country's population. Recent efforts can be seen in the 2016 United States election, as well as elections in Germany, Brazil, Canada, and more.

Through the collection of holistic data, creation of computational propaganda campaigns, and deployment of campaigns through social media, these efforts will continue to be more successful. These campaigns are often running continuously because of the rate at which information is created and shared to a network of individuals. This makes detecting and removing misinformation from the platforms difficult and time-consuming.

By identifying the significant forces involved in this complex problem, I was better able to understand the significant driving forces present. These driving forces then helped to identify potential future scenarios and significant future trends that may occur. The scenarios then led to the determination of different implications based on the outcomes of each scenario. The most notable trend that was identified is the drive to collect more information on individuals to continue to individualize the narratives in campaigns.

Background

Growth of Computational Propaganda

Computational propaganda can be found under the umbrella term Information warfare. Information warfare has been a topic of intense study since the early 1990s. It has continued to evolve since then and now includes computational propaganda as a subset of technique/method by which information warfare is waged.

Computational propaganda is a term used to define the more recent phenomenon that includes both manipulation and misinformation efforts in the digital sphere. Computational propaganda is best described by Samuel Woolley and Philip Howard (2017) as "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks." This form of information warfare differs from others because its major strength is using meta and content data to more successfully target people. From its beginning the major improvements of computational propaganda can be seen in the dissemination of messages more successfully to targeted people.

The growth of state-sponsored propaganda has "exploded with the rise of social media" and numbers from the congressional testimony of Facebook, Twitter, and Google, where more than 150 million people in the United States alone have been exposed to these campaigns (Bjola, 189). This rapid growth has become a phenomenon because of its power to be an effective, non-military technique, that achieves strategic goals, such as creating discontent within a population. The weaponization of information in computational propaganda has become the ideal tactic for enabling political change.

One of the first large-scale, successful campaigns in the United States using computational propaganda was during the 2016 United States Presidential elections. The use of bots in a number of networks and social media platforms like Twitter and Facebook, proved to be extremely successful at creating, distributing, and redistributing within echo chambers, misinformation to users. Prior to the U.S. campaign, similar efforts were also seen in the events surrounding Brexit. Since, bot networks have been identified as influencers in locations such as: Canada, Poland, Germany, and Brazil. Efforts in these locations had similar strategic goals: swaying public opinion and beliefs through false amplifiers, algorithmic manipulation, and spreading of a strategic narrative.

Current Methods

The most popular and successful method is the use of bots, which are automated programs that perform simple and repetitive tasks. It has been estimated that on social media platforms, bots consist of about 9% of their user base (Varol, Onur, et al.). These bots are often essential to the spreading of computational propaganda because they are able to perform the simple tasks that humans can do, but bots can instead do them at a much larger scale. The bots are strategically deployed in networks so that they can both collect information, as well as communicate with people in a network. The key to using bots is their ability to deploy information and news, interact with users, effect algorithms, and more, while passing as a human user. Their ability to stay within a certain activity threshold lessens the chance that a website algorithm will identify the faux account.

Bots begin their connections through the interaction with users. The bots are interconnected with each other within a separate network and feed off each other's interactions. This creates a layered effect within the bot network. Through interactions, the bots then interact with node networks. The node networks evolve with the K-core decomposition, which breaks down into separate layers and trims nodes that have the fewest connections, which intensifies it at its core. Figure 1 shows an example of the layers of within a node network. The upper core of the network usually sets the agenda for the rest of the network. Samuel Woolley and Douglas Guilbeault (2017) identify that the core of these networks have the capability of trigger cascades of recruitment during an event and reaching a lot of users. The infiltration of the bots into these networks gives the bots access to the upper echelons of influence within the entire network. An example of a network that is infiltrated with bots can be seen below is Figure 2. This is a network from the 2016 United States President election on Twitter.

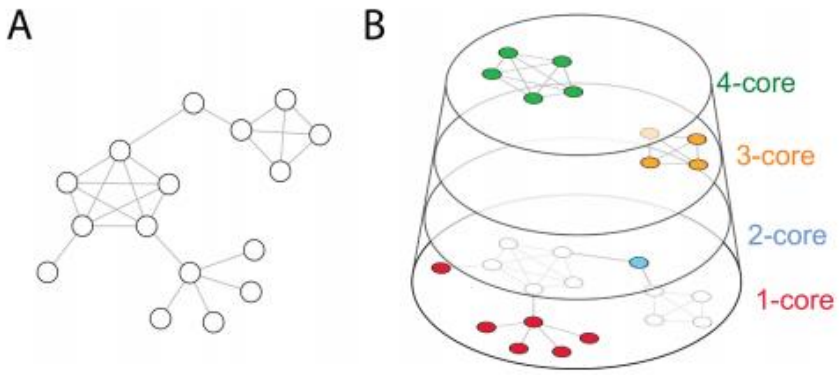


Figure 1: Graphic Illustration of K-Core Decomposition (Barberá et al., 2015)

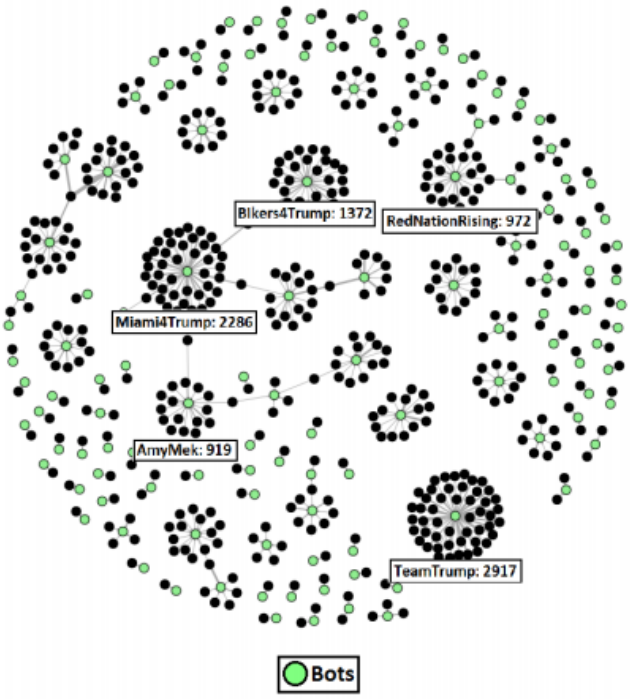


Figure 2: Directed Network of Humans Retweeting Bots with Threshold Removing All Users with Only One Connection (Woolley and Guilbeault, 2017)

The other popular method used to deploy computational propaganda is the use of trolls. Trolls are people who target groups and communities on social media platforms with hate speech, as well as online harassment (Bradshaw and Howard, 2018). Trolls do bring a unique set of narratives to the networks; however, they are not as popular as using bots to spread computational propaganda campaigns because they often can't develop a far enough reach. So, trolls have been found to be transitioning into a role that is geared more towards narration creation. Their designed narratives can then be fed into bot networks.

Capacity of Nation States and Presence of Efforts

The capabilities and current capacity of cyber operatives in nation-states is difficult to determine. However, in in the Computational Propaganda Research Project, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," both Samantha Bradshaw and Philip Howard (2018) have attempted to identify and categorize nation-states that have low to high cyber operatives present within the country. This gives a high-level overview of the capabilities of nation states and enables concerned parties to get an idea of where to focus resources and which state-actors should be focused on.

Below in Figure 3 is a global cyber troop capacity, as identified by Bradshaw and Howard (2018). This report has characterized high capacity nation states as those that have a large team and budget dedicated to information warfare and psychological operations. High capacity countries also spend a significant amount of funding on research and development and have sophisticated and a variety of techniques to use. They also operate full-time, rather than only during critical periods of time. Countries that fall within this capacity are: China, Israel, UAE, and the United States. Other capacity nation-states can be seen in the graphic below. Both high and medium cyber capacity countries should be monitored.

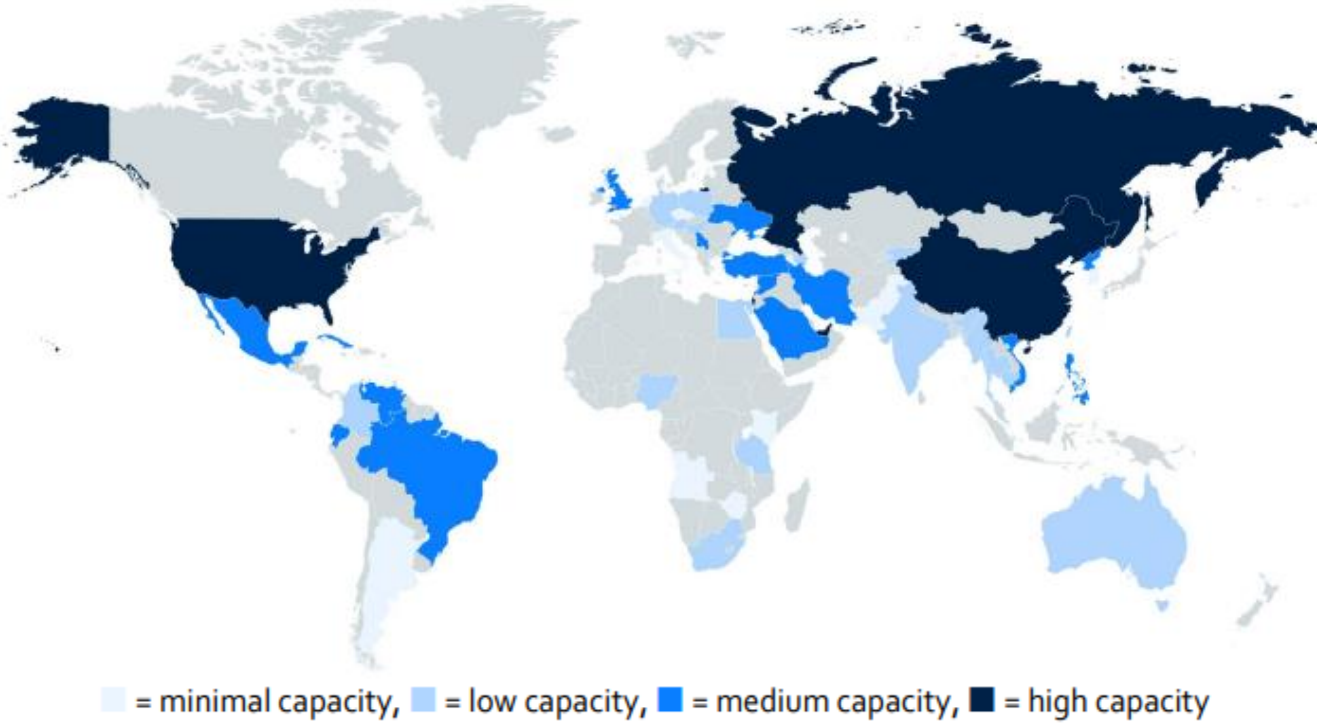
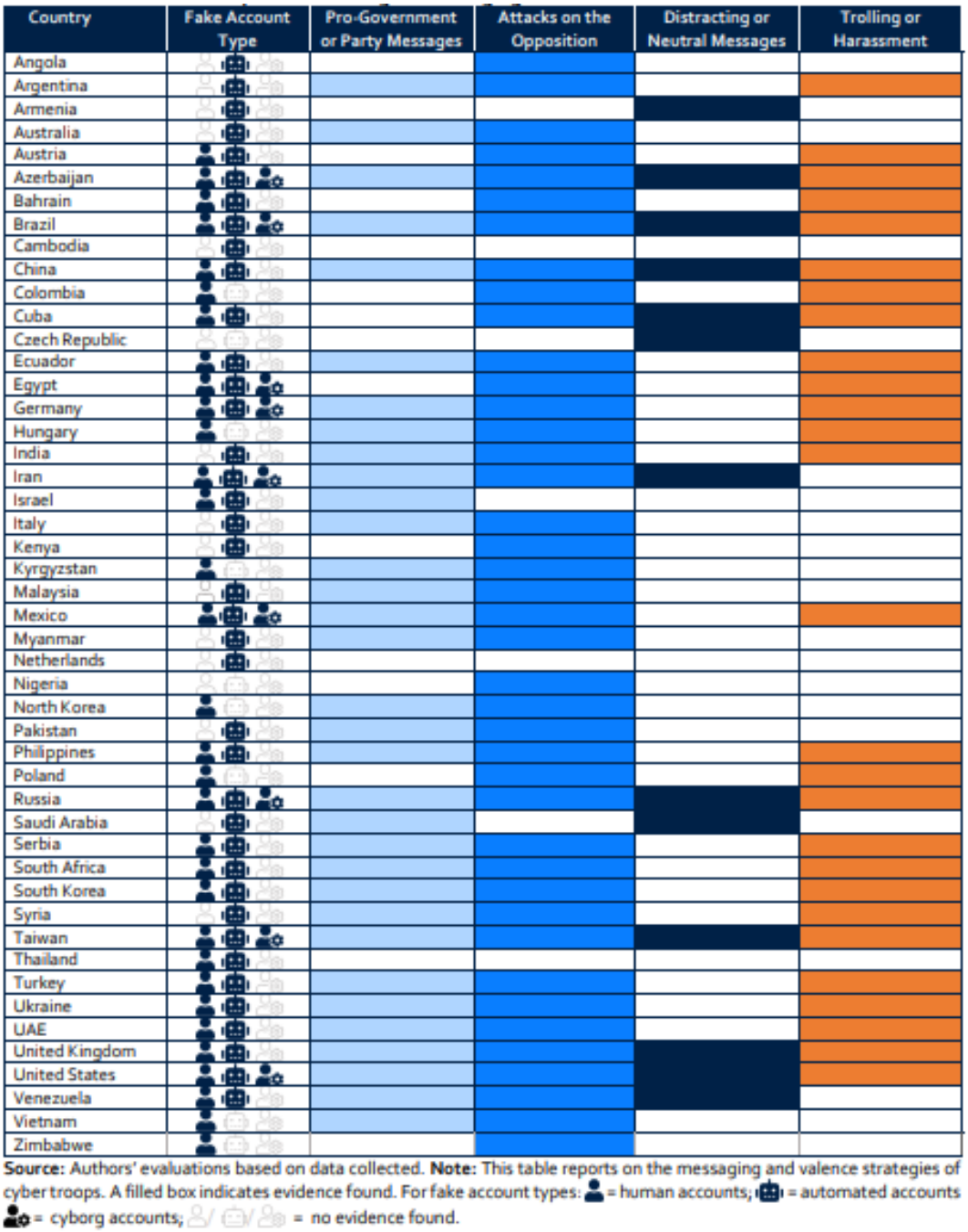


Figure 3: Global Cyber Troop Capacity in 2018 (Bradshaw and Howard, 2018)

Although these high capacity nation states have strong capabilities, what is even more interesting is Figure 4 below, which shows fifty selected countries and the presence of computational propaganda in that state. There are only a few countries that have all fake account types present, as well as the methods of messaging. These countries include: Azerbaijan, Brazil, Russia, Taiwan, and the United States. Maintaining this chart may prove essential to following trends as the presence of these various elements change over time in these countries.



Country	Fake Account Type	Pro-Government or Party Messages	Attacks on the Opposition	Distracting or Neutral Messages	Trolling or Harassment
Angola			■		
Argentina		■	■		■
Armenia				■	
Australia		■	■		
Austria			■		■
Azerbaijan		■	■	■	■
Bahrain			■		■
Brazil		■	■	■	■
Cambodia					
China		■	■	■	■
Colombia			■		■
Cuba			■	■	■
Czech Republic				■	
Ecuador		■	■		■
Egypt			■		■
Germany		■	■		■
Hungary		■	■		■
India		■	■		■
Iran		■	■	■	
Israel		■			
Italy		■	■		
Kenya			■		
Kyrgyzstan		■	■		
Malaysia		■	■		
Mexico		■	■		■
Myanmar		■	■		
Netherlands					
Nigeria			■		
North Korea		■	■		
Pakistan		■	■		
Philippines		■	■		■
Poland			■		■
Russia		■	■	■	■
Saudi Arabia		■		■	
Serbia		■	■		■
South Africa		■	■		■
South Korea		■	■		■
Syria		■	■		■
Taiwan		■	■	■	■
Thailand					
Turkey		■	■		■
Ukraine		■	■		■
UAE		■	■		■
United Kingdom		■	■	■	■
United States		■	■	■	■
Venezuela		■	■	■	
Vietnam		■	■		
Zimbabwe			■		

Source: Authors' evaluations based on data collected. **Note:** This table reports on the messaging and valence strategies of cyber troops. A filled box indicates evidence found. For fake account types: = human accounts; = automated accounts = cyborg accounts; = no evidence found.

Figure 4: Social Media Manipulation Strategies: Messaging and Valence (Bradshaw and Howard, 2018)

Differing Opinions on Computation Propaganda

During research, several different opinions on computational propaganda, its effectiveness, and how it may or may not be used in the future, were identified. With propaganda having a long history of use throughout the world but being used via media and electronic device being more recent, an interesting dichotomy of conversations have begun on the topic. For this project, a number of different sources were reviewed such as: scholarly articles, books, newscasts, news articles, research and thinktank reports, and intelligence reports.

The most widely discussed narrative found in the sources used was the use of computational propaganda in order to spread misinformation. This tactic can be seen in the more recent 2016 Presidential election, where Russia was accused of spreading false news and misinformation through the use of bots on social media networks. Most intelligence reports, such as "Assessing Russian Activities and Intentions in Recent US Elections" (2017), identify that Russia's goal through this campaign was to undermine democracy. The Computational Propaganda Research Project has released a number of reports and summaries on the topic. These reports identify computational propaganda as a continuously growing concern. The reports identify that social media is the main platform for campaigns because of how effective it is in spreading the propaganda.

Despite the growing concern regarding the topic, many intelligence reports that outline threats to be aware of, do not discuss computational propaganda in great length. Often, it is simply lumped into cyber threats and not truly addressed. The "Worldwide Threat Assessment of the U.S. Intelligence Community" (2018) briefly outlines their concerns with cyber propaganda. However, they mostly discuss their following of cyber issues as directly related to physical repercussions such as electrical grids, government intranet. Similarly, the "Department of Defense Cyber Strategy" (2018) does not discuss the computational propaganda treat at all.

Although threat reports do not stress the significance and the potential impact that computational propaganda will have, a number of think tank and research organizations have started to release general threat reports on the topic. The Oxford Internet Institute, in a number of reports such as "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation" (2018) and "Computational Propaganda in the United States of America: Manufacturing Consensus Online" (2017), the growing presence of cyber propaganda efforts is stressed. The Institute believes that as the presence and effectiveness continue to grow, there is also an increasing threat to democracy.

The most popular narrative that can be found is that most believe social media to be the continued platform for deployment of propaganda and that narratives within campaigns continue to become more focused on people based on their beliefs and ideologies. Often individuals and/or groups are targeted that have a more polarized set of beliefs.

This literature review highlights the differing opinions on computational propaganda, how it has been used, its effectiveness when it has been deployed, and what this means for the future. This report is a synthesis of conventional wisdom on the topic and new ideas, which brings unique information to consider when using analytical methodologies.

Scope of Information Used

This topic is complex to comprehensively understand and tackle. However, to better understand the data collected and to weigh the validity of the sources, a quality of information check was performed using the "Structured Analytic Techniques for Improving Intelligence Analysis" (2009).

The first step of the check was to systematically review the sources collected and used to ensure their accuracy and minimal bias. Most sources collected are ranked as experts in the field and originate from academic journals or government produced documents, so the sources were found to be accurate. It should be acknowledged that some potential bias may be present, however it is nominal. When a larger presence of bias in documents was identified, the information was collected and noted as biased in order to ensure that the analysis was conducted on high quality, objective information. It was essential to the project to collect quality information to then analyze and provide a value added to the field, past the conventional wisdom and assessments already present.

After collecting sources and information, sources that were either compelling, or critical, or both, were identified. These sources then became the foundation for the analysis. Reports by think tanks, research centers, and other universities were the primary sources of information. After reviewing these reports, analytic techniques were then used, such as key assumptions checks, red team, causal analysis, and others.

One weakness in the data on this topic is the lack of quantitative data that can be accessed through open source avenues and in general. Additionally, the quantitative effectiveness or ineffectiveness of propaganda efforts can be hard to determine until sometime after the campaign has ended, if at all. It can also be difficult to discern between propaganda efforts and other factors present at the time. As noted before, this is a complex topic and can become very interconnected.

The quality of information check also encouraged for a consideration of any and all ambiguous sources that may be providing confusing and/or ambiguous information. There were a couple instances of ambiguous source information, such as information that was discussing both influence operations and cyber warfare. Often these terms get lumped together as one entity, however they are different from one another. Thus, when used incorrectly it can be difficult to understand what an author may be saying. In instances such as this, the source was either disregarded or considered on a minimal basis.

A moderately high level of confidence is justified in the underlying sources, given their quality, validation in the field, and the comprehensive research conducted in their conclusions. While some of the information gathered was identified with some bias, these sources were further examined to avoid strong biases. By using this data in the analysis, conventional wisdom can be challenged, and value and insight can be added to the discussion.

Analysis

Causal Forces

To achieve a greater understanding of the causal forces involved with worldwide computational propaganda efforts, a causal model was created. Using this model, the most significant forces in the system can then be identified and extrapolated. Below in Figure 5 is the causal model for this assessment.

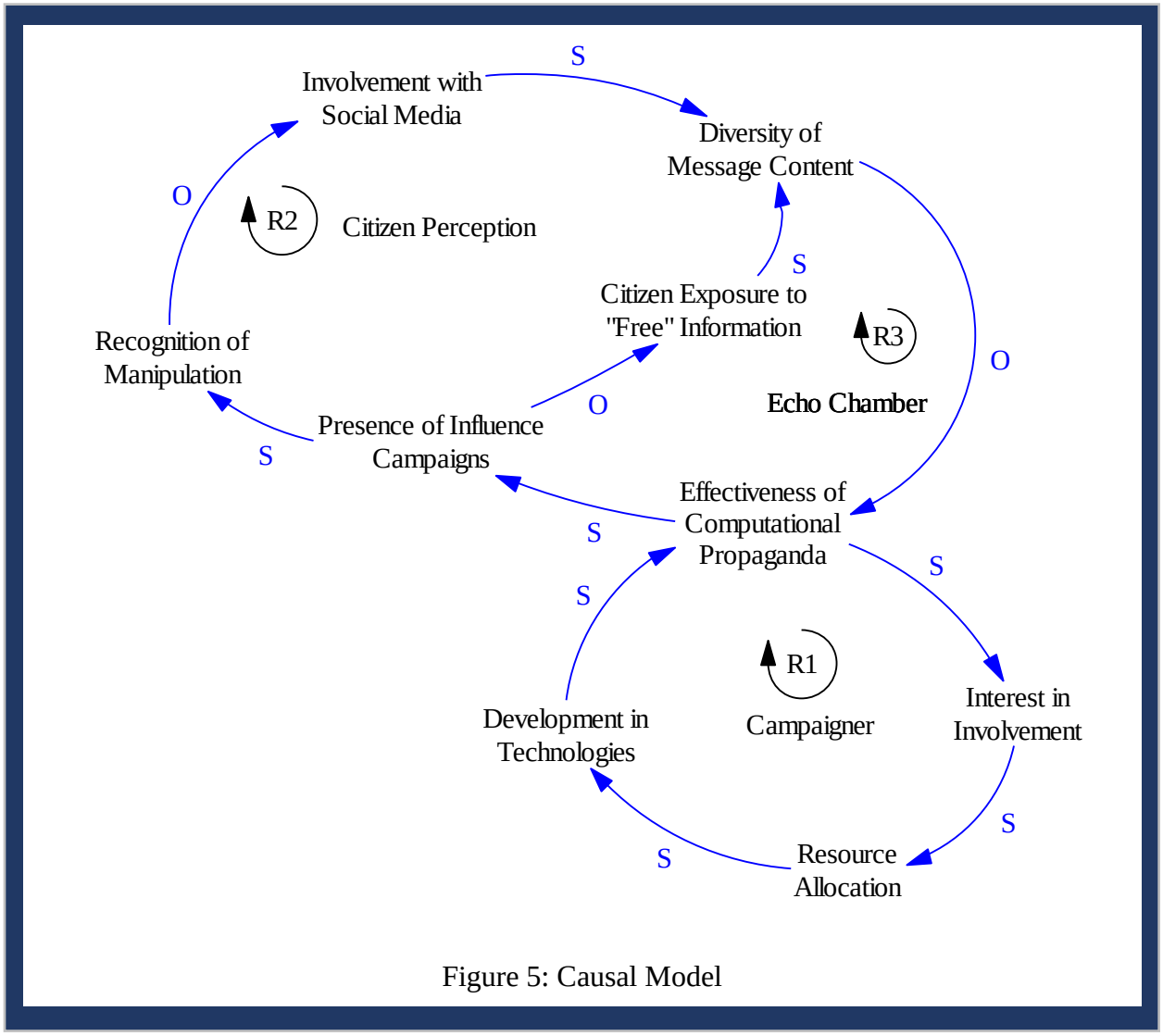


Figure 5: Causal Model

In this causal model, there are three major relationships that have been identified in this complex system. The first is labeled “Campaigner” and is R1, meaning that it is a reinforcing loop. This loop captures the entities that are using and/or attempting to use computational propaganda techniques and methods. This loop shows that the entities, both state and non-state actors, continue to invest in computational propaganda as long as it continues to be effective. This means that they will also continue to invest in new and improved ways to be more and more effective. The next loop is labeled “Echo Chamber” and is R3, meaning that it is another reinforcing loop. This loop

demonstrates how individuals will likely continue to interact with many of the propaganda campaigns because most prefer to interact with content that is similar to their views and beliefs. This creates echo chambers as individuals continue to only interact, such as sharing, "liking", etc. with content that they agree with. The last loop is labeled "Citizen Perception" and is R2, which means that this is another reinforcing loop. This loop shows how citizens interact with propaganda efforts. This causal loop has three reinforcing loops meaning that these forces, when interacting with each other, have the opportunity to spiral out of control and continue to occur or have the opportunity to be rejected and then continue to be rejected.

Scenario Futures Generation

The drivers used in this futures assessment were derived from the causal forces model. When selecting scenario drivers, three causal variables that were most uncertain and most significant, were identified. These drivers include: 1) the content of a message or narrative, which can be more narrow or more broad, 2) Technological development in this space, which either continues or begins to stagnate and transition to technological developments in a different sector, and 3) the public's reaction to influence campaigns, which they can either largely accept or reject. The drivers can be found in the quadrant matrix in Figure 6. These scenarios will be expounded upon in the next section of this assessment. The authoritative, alternative, and exploratory scenarios can be found in the main section of this assessment, and the other five scenarios can be found in the "Methodologies" section at the end of the assessment.

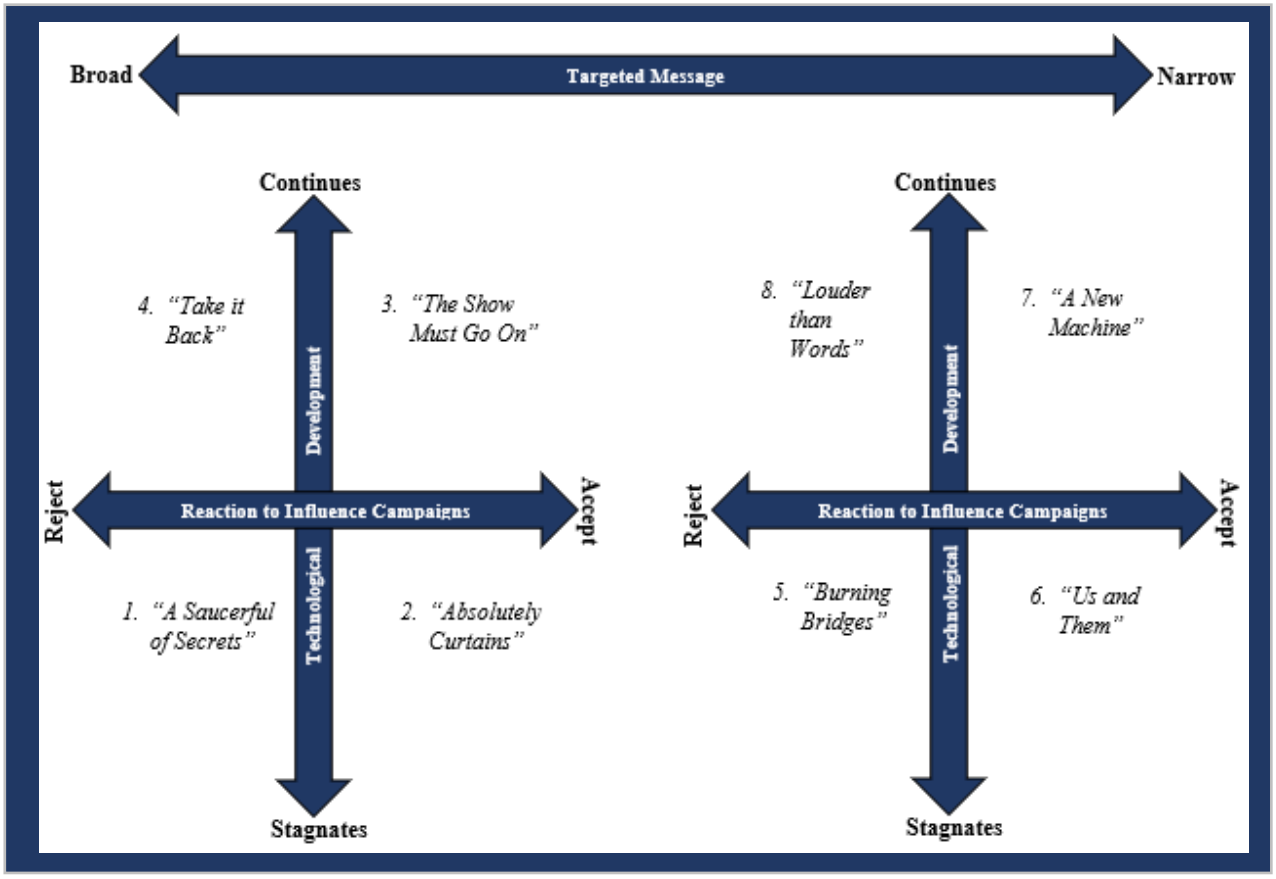


Figure 6: Scenario Quadrant Generation

Authoritative Assessment

The authoritative assessment represents the likely future outcome as a result of interactions between significant forces and trends. This is scenario seven, titled "New Machine." By extrapolating the significant forces, we were then able to generate scenarios and development them to understand their potential future impact and the implications of those impacts. This scenario suggests likely events that may occur as we approach the ends of the quadrant matrix for this scenario.

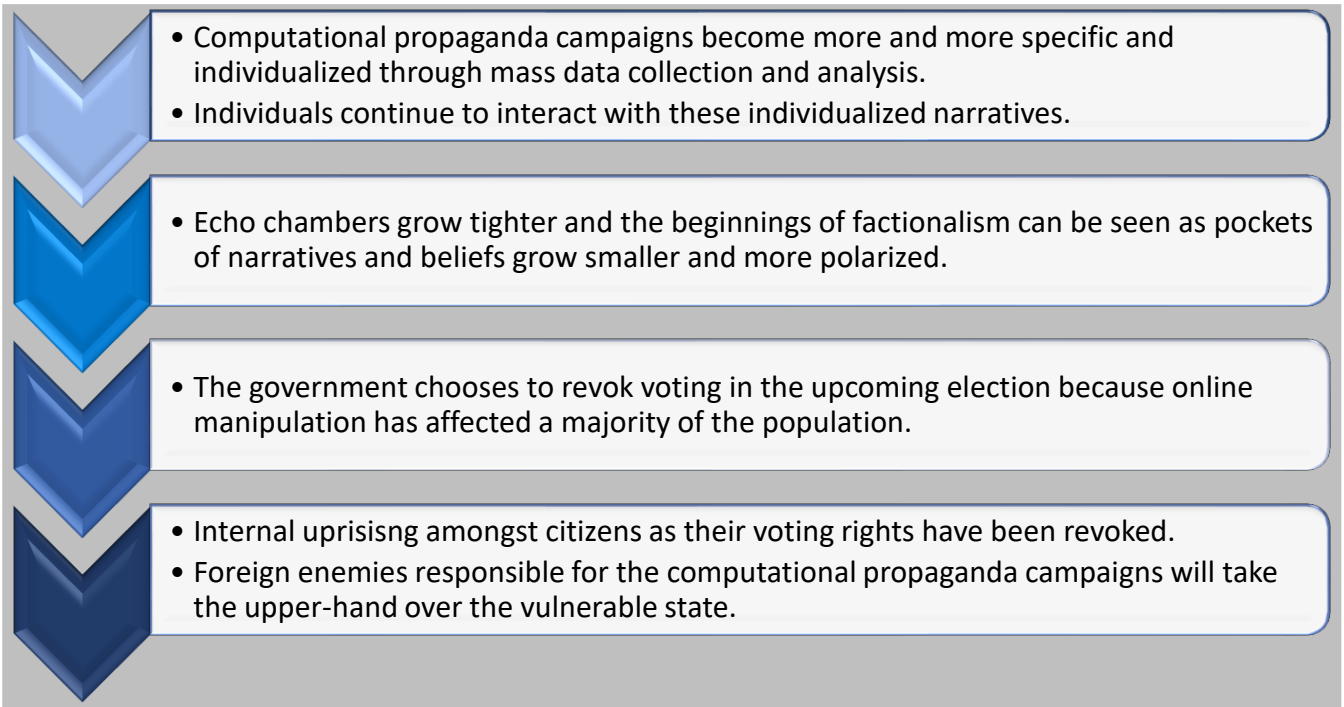


Figure 7: Hypothetical Timeline for "New Machine"

Technological developments continue to occur at high rates; Messages being targeted to people have become narrowly focused; and individuals have an accepting reaction to influence campaigns being conducted.

State and non-state actors find more and more success with their propaganda campaigns on social media platforms and other places on the internet where individuals are interacting with both media and each other. However, as strategic goals of this organizations continue to change and become more and more specific, the content for the propaganda must also change. Additionally, entities are finding that, although people continue to share fabricated narratives, the effect of those narratives has started to lessen.

Using sophisticated algorithms, smart devices, and other technological mediums that allow for data collection, entities begin to collect more data to analyze on individuals within a society so that more directed and specific narratives can be created and deployed. These narratives begin to create hyper-specific groups and tightly-knit echo chambers, which causes polarization of people in greater numbers. This starts to lead to the beginnings of factionalism.

People are being fed information that they agree with, so they want to see more of it and want to continue to interact with it. They share it on their platforms, which, after some time, starts to create a lot of tension between individuals. The social media platforms that once were a location for keeping in touch with family and friends, starts to turn into an online battlefield with individuals attacking others for sharing their polarized views.

This online behavior begins to transition and take form in everyday life. People at their workplaces pull away from each other and/or interrogate each other over their differing views. This continues into friends and family spheres and also at increasing rates. As elections and other critical power shifts in the government grow near and the public falls further and further under the influence of propaganda and influence campaigns, the government struggles to figure out the best course of action. They determine that allowing people to cast their influenced-charged vote, will ultimately result in a victory for a foreign entity. So, voting rights in the upcoming election are revoked until these campaigns can be thwarted.

This decision results in a total uprising from the public as the core of their democratic values have been revoked and the foundation upon which the current government was built crumbles. Democracy will cease to exist, at least now, in the country as the government has essentially taken the side of a totalitarianism. During this breaking point within the state, the foreign entity/entities responsible for the propaganda campaigns will have the opportunity to gain the strategic advantage and will be able to take the upper-hand as the state continues to face major internal turmoil.

<u>Notable Implications:</u>

- Data collection reaches extremely high rates as entities are collecting data on individuals on a number of different platforms, from different devices, and have scaled their collection efforts up.
- Echo chambers will have very specific messages and less members, however there will be more echo chambers. This is the creation of factionalism within the state
- Democracy will fail as the core democratic rights are revoked in order to “save” the state from foreign intervention.
- Total uprising within the state will take place as there is a major pushback from citizens as a result of the government’s decision.
- Foreign enemy/enemies will have the opportunity to take the upper-hand as the state is extremely vulnerable.

Alternative Assessment

The alternative assessment represents the plausible outcome as a result of interactions between significant forces and trends. This assessment is based on forces that are influential to the system. However, there significance/impact, as well as probability of occurring is less than the authoritative assessment. Again, indicators of change were identified, and unintended consequences were considered.

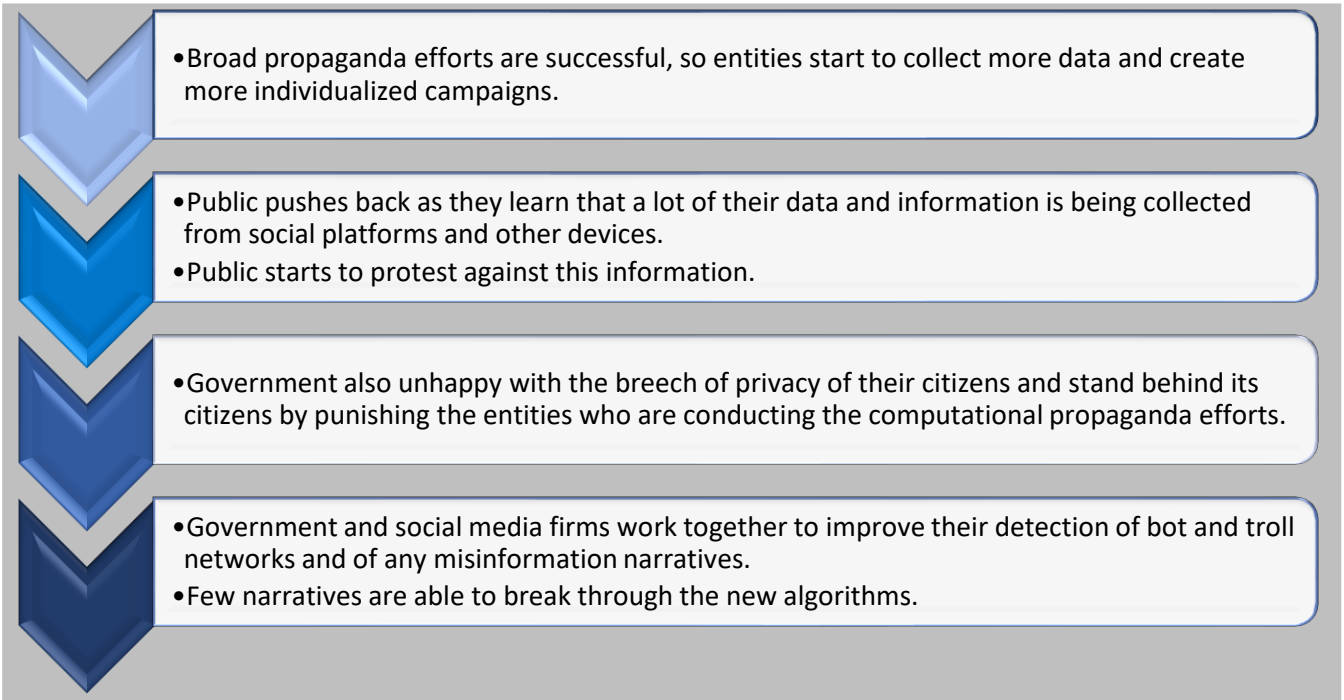


Figure 8: Hypothetical Timeline for "Louder than Words"

Technological developments continue to occur at high rates; Messages being targeted to people have become narrowly focused; and individuals react to influence campaigns being conducted by rejecting them.

Computational propaganda efforts found a lot of success in the early stages of its campaigns. As a result, entities continued to push for more campaigns. Through the collection of data on individuals from the social media platforms and other devices, entities are able to create highly individualized narratives to present back to the public. They create these in hopes that they can continue to divide the public in their perceptions of their current government. However, this collection of data and invasion of privacy becomes a concern to a number of individuals who then relay this information to the rest of the public.

Information is released from social media firms and other organizations who have been involved in this collection of data confirming that big data has been harvested from their devices and networks by the entities that are conducting the misinformation operations. The public is outraged because they value privacy very highly. The public, even though they may agree with

the messaging they have been receiving, begins to pushback against the narratives that they are being presented with.

The government recognizes the breech of data collection on these platforms and also pushes back on the foreign entities believed to be conducting the computational propaganda. The public and government start to unite under a single front against the entities conducting the operations. Although the public started to grow skeptical of their own government's intentions at the beginning of the propaganda campaigns, the recent backing of public concerns has created a new sense of trust between government and public.

The government does what it can to fight back against those conducting the operations through means such as sanctions, breaking of relations, etc. This limits the ability for them to continue to conduct operations. Additionally, the government and the organizations that were being used to propagate the propaganda work together to improve algorithms and identification methods of bots, trolls, and misinformation.

Notable Implications:

- Tensions between government and public lessen as both bond together to fight against the misinformation campaigns.
- Improvements made in detection and thwarting of efforts, bot and troll networks, and deletion of all misinformation narratives.
- Little propaganda efforts can make it through the new detection algorithms.
- Foreign entities conducting operation shift their focus back to cyber operations that can threaten physical intranets, electrical grids, etc.

Exploratory Assessment

The exploratory assessment represents the potential outcome that results from a high impact/low probability scenario. This outcome is important to identify and understand because, although unlikely to occur, it has potential consequences that are too significant to disregard.

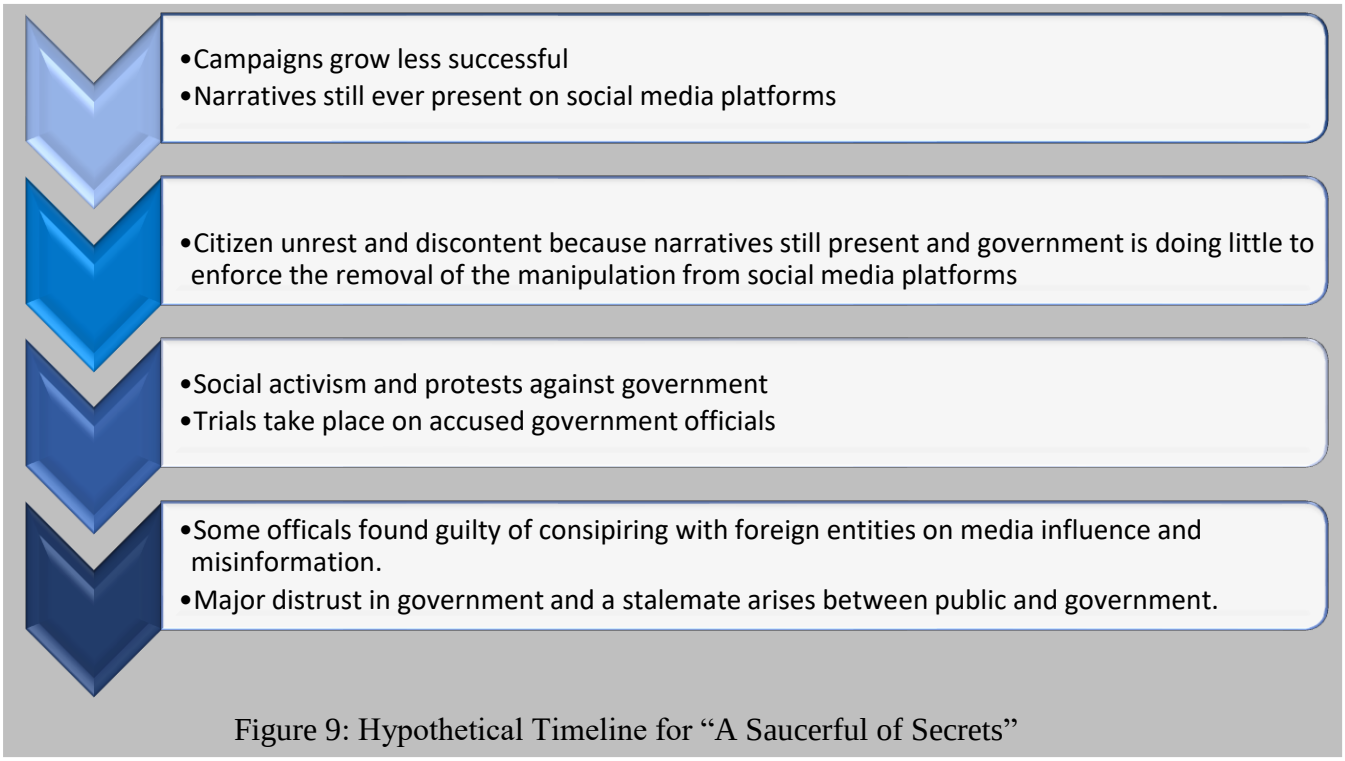


Figure 9: Hypothetical Timeline for "A Saucerful of Secrets"

Technological developments begin to stagnate and move slower to develop and disseminate; Messages being targeted to people remain broad; and individuals react to influence campaigns being conducted by rejecting them.

Computational propaganda campaigns found some success early on in various countries, however they continue to become less and less effective as the narratives and messages that once divided society become less important and "yesterday's news." However, entities continue to push the narratives that have been successful in the past, hoping that they will again gain some traction. Still, nothing seems to take traction.

An intolerance for these campaigns starts to come out of citizens as the same messages continue to get pushed and little to nothing is being done to stop these campaigns. People grow tired of seeing them every day on their social networks when most people just want to interact with friends and family without seeing politically charged propaganda every day.

A wave of activism and rallies starts to form in protest of these narratives flooding their networks and they begin to protest the social media firms for doing little to nothing to remove the messaging and the government for not holding the social media firms more accountable to ensuring that these bots, trolls, and their narratives are removed immediately.

Speculation starts to grow in the unhappy citizens that the government is actually part of the manipulation that is still present because of their lack of effort in removing the narratives. There is call for new government officials, because the public believes that the current officials are working against them and/or with the enemy state to manipulate them, begins. As these accusations begin, investigations are launched on government officials that are accused of conspiring with foreign entities on manipulation and influence campaigns that may have helped them into power.

Accusations come to light as being true and several government officials are tried with essentially conspiring against the population because of the efforts put into mass manipulation and creating social divides that enabled their election into a government position.

The recent news has caused the public to have an extreme amount of distrust in the government. This pushes democracy to its seams as the public is unsure how to proceed, not accepting that the government is now moving forward with democratic values instilled in the system again. A stalemate is seen between the public and the government and relations grow tense, but both parties are unsure what to do moving forward. This takes the focus away from outward issues as the internal essence of the country has been compromised. Thus, foreign enemy entities are able to take advantage of these vulnerabilities.

Notable Implications:

- Protesting and major pushback coming from the public because of their beliefs—that the U.S. is involved in the manipulation schemes.
- Democracy cracking at the seams as there is major vulnerabilities in current government and trust in the government from the public.
- Stalemate between government and public gives foreign enemies the opportunity to gain the upper hand as the government is focused more inward.

Mitigation Strategies

As a result of computational propaganda being fairly new, most countries that have been affected by it have not yet made any advancements or taken any actionable move towards trying to defend against this threat long-term. In several reports focusing on this topic, there have been a number of mitigation strategies discussed that may help to lessen the effect of propaganda campaigns in the cyber domain. In "Computational Propaganda Worldwide: Executive Summary," the authors call to social media firms to better design for democracy and for governments to help back them when making necessary changes. By redesigning their platforms, social media organizations can better promote political news and information from reputable sources. This will help with restoring trust in social media systems.

Organizations must also start holding social media firms accountable to stronger data collection laws and being vigilant in identifying and removing faux accounts. The collection and analysis of accounts on Facebook was one of the reasons that Russia was able to create the narratives and deployment strategies during the 2016 U.S. Presidential election. Holding social media firms more accountable for all successful bot penetration on their platform may encourage them to put more effort into identifying bot and troll networks and moving to remove them.

Improved public education and better understanding of the topic will also help to teach people how they can avoid falling for the misinformation and influence campaigns that are being spread. Computational propaganda campaigns only thrive in an environment that is a low-trust, where anything can be said and shared. So, giving people improved skills on how to identify these campaigns will increase the likelihood that they will spot these campaigns on their social media platforms. One way to educate the public could be publicly exposing trolls and bots, as well the internal workings of a campaign to show them examples of what each may look like.

One last major mitigation strategy that could lessen the impact of this system is, at minimum, a conversation about creating policies and regulations for bots. Bots are a huge reason why computational propaganda campaigns are so successful. They are able to perform complex algorithms and identify ideal pockets to input a certain narrative and they can do this at a scale that a troll cannot keep up with. Currently, bots are able to thrive on most social media sites because these sites have lax API access. Currently, there is very little discussion going on within the U.S. government regarding potential policies and regulations for bots. The only acknowledgement to the topic is the US Anti-Bot Code of Conduct (ABCC), where U.S. government representatives, as well as individuals from major ISPs gather to talk about all kinds of bots. We need this discussion to open and to grow, as well as for groups like this to start bringing policies to the table so that we can move from conversation to action.

Conclusion

After examining a number of future states generated using Alternative Futures Analysis, ranging from more likely to less likely, as well as more significant to less significant, a number of shared themes were identified within these futures. Additional themes and trends were identified conducting the early causal analysis model. First, misinformation and computational propaganda proves to be a powerful tool against democracy and entities against democracy are using this tool more and more all over the world. Examples of use and success can be seen in the United States, Brazil, Poland, Canada, Germany, and more.

Second, the efforts by entities conducting the campaigns are growing stronger and are adapting to the responses being made by countries affected by the campaigns. Actors have been found to be adapting their automation in response to the research and media coverage about the topic. Thus, the bot and troll networks, as well as the misinformation that they release is becoming more difficult to identify. They have also adapted their troll and bot networks to fall under the threshold of identification because they have adapted, knowing what the threshold is for most social media platforms, and remaining active, but not active enough to alarm the detector.

Social media will continue to be a location for computational propaganda efforts as most citizens are involved in at least one of the social media firms. These platforms are not only popular, but also provide entities the opportunity to segment audiences and target messages in quick and cheap ways. The echo chambers and factions being created have caused a noticeable divide in the public and this is seen as the first success to those conducting the operations. Entities will continue to pray on these divides as it enables them to continue to underscore democracy and push citizens to reject it outright.

We have entered a new era of influence and propaganda. What was once broadly-themed posters have now transformed into targeted messaging with both long-term and short-term strategic goals in mind. Thus, we need to improve methods and strategies to counter these computational propaganda efforts. In identifying current and potential trends regarding this topic and the implications of those trends, we can better prepare the and construct defensive measures against future operations, especially as the adversaries change and the landscape evolves.

There is a moderately high level of confidence in this assessment. This confidence level does not echo the likelihood of any single outcome, instead it is derived from the combination of research on past and current trends, relationships, and history, as well as the methodologies used to analyze that information. The check on assumptions, quality of information and sources, the robust methodologies used, and the medium level of denial and deception present also contribute to the confidence level of this assessment.

Bibliography

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65-88.

Al-khateeb, S., Hussain, M. N., & Agarwal, N. (2017, July). Social Cyber Forensics Approach to Study Twitter's and Blogs' Influence on Propaganda Campaigns. In International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation (pp. 108-113). Springer, Cham.

Barberá, P., Wang, N., Bonneau, R., Jost, J. T., Nagler, J., Tucker, J., & González-Bailón, S. (2015). The critical periphery in the growth of social protests. PloS one, 10(11), e0143611.

Bjola, C. (2017). Propaganda in the digital age. 189-191.

Bolsover, G., & Howard, P. (2017). Computational propaganda and political big data: Moving toward a more critical research agenda.

Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: a global inventory of organized social media manipulation. Computational Propaganda Research Project, Oxford Internet Institute and University of Oxford. July, 20.

Bradshaw, S., & Howard, P. N. (2018). The Global Organization of Social Media Disinformation Campaigns. Journal of International Affairs, 71(1.5), 23-32.

Central Intelligence Agency, Center for the Study of Intelligence. (2009). A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis.

Coats, D. R. (2018). Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence.

Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber Threat Intelligence: Challenges and Opportunities. Cyber Threat Intelligence, 1-6.

Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., ... & Quattrociocchi, W. (2016). The spreading of misinformation online. Proceedings of the National Academy of Sciences, 113(3), 554-559.

Geers, K. (2011). Sun Tzu and cyber war. Cooperative Cyber Defence Centre of Excellence, February, 9.

Howard, P., & Bradshaw, P. (2017). Troops, trolls and troublemakers: a global inventory of organized social media manipulation.

Howard, P. N., & Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence.

Lewandowsky, S., Ecker, U. K., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the “post-truth” era. Journal of Applied Research in Memory and Cognition, 6(4), 353-369.

Lindqvist, U., & Neumann, P. G. (2017). The future of the Internet of Things. Communications of the ACM, 60(2), 26-30.

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. Journal of Cyber Policy, 3(1), 39-43.

Morozov, E., & Docksai, R. (2011). Technology's role in revolution: Internet freedom and political oppression. The Futurist, 45(4), 18.

Office of the Director of National Intelligence. (2017). Assessing Russian Activities and Intentions in Recent US Elections.

Sanovich, S. (2017). Computational Propaganda in Russia: The Origins of Digital Misinformation. Working Paper.

Shao, C., Ciampaglia, G. L., Flammini, A., & Menczer, F. (2016, April). Hoaxy: A platform for tracking online misinformation. In Proceedings of the 25th international conference companion on world wide web (pp. 745-750). International World Wide Web Conferences Steering Committee.

Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., & Menczer, F. (2017). The spread of fake news by social bots. arXiv preprint arXiv:1707.07592, 96-104.

The Department of Defense. (2018). The Department of Defense Cyber Strategy. The US Department of Defense, Washington, DC.

Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online human-bot interactions: Detection, estimation, and characterization. arXiv preprint arXiv:1703.03107.

Woolley, S. C., & Guilbeault, D. R. (2017). Computational propaganda in the United States of America: Manufacturing consensus online. Computational Propaganda Research Project, 22.

Woolley, S. C., & Howard, P. N. (2017). Computational propaganda worldwide: Executive summary. Computational Propaganda Project.

Methodologies

Key Assumptions Check

A key assumptions check is used to identify the judgements that are/have been made in all sources (news, reports, academia, etc.), as well as your own assumptions on the topic. Additionally, to conduct an additional assessment of those judgements to ensure that the assessment does not rest on flawed premises and to uncover any hidden assumptions that may not have been identified at the start.

There were several key assumptions that were analyzed in this report. After conducting research and the beginnings of the analytic techniques, several key assumptions were assessed. Through this assessment, several assumptions were rejected, and some were accepted. In performing this check, one can better understand the current narrative on the topic, as well as uncover more assumptions and make additional assessments.

Many of the assumptions that were made at the beginning and during the research of the topic was information that came from new sources and governmental reports, however using technical reports and think tank reports, a more accurate understanding of the original assumption was identified. This enables moving forward with the report with a more accurate understanding of the topic.

Assumption	**Assessment**
Computational propaganda campaigns are the same as misinformation campaigns.	Misinformation can be identified as a branch under computational propaganda. There are several branches that can fall under this term. These branches represent the different methods that can be used.
Propaganda efforts are only deployed through the use of bot networks.	Although this is a very popular deployment strategy, there are still people that conduct some of the creation, deployment, and monitoring of computational campaigns.
The United States is the only victim of computational propaganda.	Although the United States did suffer and continues to be involved with these efforts, a number of other countries around the world are also falling victim to these campaigns. For example, Brazil, Germany, and Canada are all examples of countries that have also experienced the effects of computational propaganda.
Social media is the only place that entities are releasing their propaganda.	Partially true. Right now, most of the campaigns are taking place on social media platforms like Facebook and Twitter. However, efforts are starting to enter other spaces like Youtube as well.

Figure 10: Assumptions Check on Russia's Involvement/Influence

Scenario Narrations (Continued)

The full alternative future scenarios generation table can be seen on page 14 in Figure 6. The following scenarios are those that were developed, but not to the extent of the authoritative, alternative, or exploratory scenarios.

2. "Absolutely Curtains"

Technological developments begin to stagnate and move slower to develop and disseminate; Messages being targeted to people remain broad; and individuals have an accepting reaction to influence campaigns being conducted.

As technological advancements in this field begin to slow, people continue to use the same social media platforms and not many changes can be seen in developing and improving propaganda campaigns on these platforms. These campaigns are very bland and very vaguely continue to poke at problems within the democratic state. Citizens are able to coexist with these computational propaganda campaigns and interact with them. However, the level at which the campaigns are deployed does not pull at the seams of democracy, so little change can be seen.

Eventually efforts in this domain slow and drop off. The campaigns were not disruptive enough to create a rift in societies and as they grow less effective, entities discontinue the use of them, at least for now. As a result, a stronger and bolder focus is placed on cyber and electronic efforts related to physical disruptions, rather than social disruptions.

<u>Notable Implications</u>

- Computational propaganda shifts in importance and a stronger focus is placed on physical disruption using technology rather than a social disruption.
- Computational propaganda falls from the cyber scene and will likely make an appearance again but is not found on platforms as strongly anymore.
- Democratic values do not diminish as a result of influence campaigns.

3. "The Show Must Go On"

Technological developments continue to occur at high rates; Messages being targeted to people remain broad; and individuals have an accepting reaction to influence campaigns being conducted.

Technology continues to develop across the globe. Cities have become a hub for convenience with technologies as these technologies continue to make life easier for people by understanding exactly what they want and need. People interact with these technologies every moment of every day and whether they consciously know that are or not.

Entities conducting computational cyber campaigns are and do collect data from these devices when they can. Although a more focused narrative could be used in their campaigns, they choose to keep a broad message. The past has shown, seen in examples of the Soviet era, etc. that manipulation via the masses is easier and cheaper. Additionally, by distributing a broad message

to everyone, they are able to stay "under the radar" when conducting these operations because a targeting message would raise too many flags.

Individuals, for the most part, are accepting of a broader, generalized message, or those who aren't truly accepting of it at least tolerate it. These broad messages are still attempting to further the goals of the entity conducting the operations, however its broad narrative makes it difficult for a strong, goal-driven narrative. Thus, entities are not able to further their critical strategic goals as well as they could. However, they continue to keep narratives broad and try to find different ways to improve their technique such as deployment of the narrative. This method is simply easier and does not cause an upset and that is valuable to the entity.

Notable Implications

- Message received is not radical or individualized enough to allow for a lot of headway for the strategic goals of the entity conducting the operations.
- Opportunities for data collection on individuals is present, so vulnerabilities could be present and the opportunity for a switch to a narrow message is present.
- Broad message, although not always extremely effective, could lead to the development of some echo chambers of large, sweeping ideals.
- Democratic values are challenged and may lead to stronger tension between people and state.

4. "Take it Back"

Technological developments continue to occur at high rates; Messages being targeted to people remain broad; and individuals react to influence campaigns being conducted by rejecting them.

Technology continues to develop across the globe. Huge advancements in IoT, computer technologies, and larger machinery like cars, etc. are made. Although these technological advancements have made collecting data on individuals significantly easier, which could then result in a detailed analysis done on each person, entities conducting computational propaganda have continued to keep a broad message because it is easier and more cost effective.

Individuals interacting with this content have grown more and more discontent because everything that is being presented to them is very vague and has little to no substance. Additionally, the identification of these attempts was made easier because of the simple, but sharp narratives. Although there was a time that this messaging was successful in creating echo chambers, social media platforms have been required to identify any and all attempts and to thwart them as quickly as possible. Thus, most messaging isn't reaching most users, but the messages that do aren't effective and are not successfully undermining the democratic values within the population.

Notable Implications

- Shift to other media platforms as a way to escape the continued campaign efforts.

- Lack of polarized narratives means that there is little additional divide seen between members of society.
- Altercations between governments as the campaigns continue unsuccessfully, but the foreign entity is unwilling to accept responsibility for efforts and/or discontinue efforts.

5. "Burning Bridges"

Technological developments begin to stagnate and move slower to develop and disseminate; Messages being targeted to people become narrower and more individualized; and individuals react to influence campaigns being conducted by rejecting them.

Pressure begins to build on foreign entities to make a change in their status of power in the world. The computational propaganda campaigns have proven successful in the past, but they want to ramp up efforts so that they can start seeing results quick. Using only the algorithms and bots, these actors start to narrow and focus the narratives that are being deployed, however they are seeing more and more pushback of these narratives because they are not being introduced to the right individuals. Although the algorithms were somewhat successful in developing narratives, they are not sophisticated enough to also determine the right pocket of individuals to deploy the hyper polarized narratives to.

The push for narratives on social media platforms becomes very obvious as clear messaging efforts can be identified since they are very specific. This leads to further pushback from the public because they are angry that these messages continue to break through on the platforms. People start to leave their social networks, angry that the messaging continues when they simply want to connect with friends and family. As campaigns become less and less effective, entities start pulling back and regrouping.

<u>Notable Implications</u>

- Push back from public on social media firms as clear messaging is continuing to break through via bots and trolls. People start to move away from the social media platforms that continue to allow misinformation messaging to occur.
- Uniting of public, more so, against the manipulation efforts.
- Computational propaganda efforts slow tremendously and start to edge back towards a broad narrative again in hopes that these tactics can prove to be successful again.

6. "Us and Them"

Technological developments begin to stagnate and move slower to develop and disseminate; Messages being targeted to people become narrower and more individualized; and individuals have an accepting reaction to influence campaigns being conducted.

There is a lot of success in the current computational propaganda efforts and entities continue to use algorithms and bots to identify potential message narratives and individuals to receive the misinformation on social media platforms. Slowly, as echo chambers and factions are created

within the social sphere, entities begin to narrow and alter their message to better fit their ultimate strategies and goals. Because the public has been so accepting of the messaging and their unhappiness with their current government continues to grow, they are also accepting of the new, more individualized narratives being presented to them.

The entities conducting the misinformation campaigns are able to further divide the public because of the trust that they have built with the public and the distrust that they have caused the public to have with their own government. This leads to major tension between the government and the public as democratic values are being undermined because the public believes that they no longer have a say in the innerworkings of the government (part of the narrative that they have been fed from the outside entity).

Notable Implications

- Tension between public and government causes issues in future elections because the public believes that it can no longer trust their government.
- Democracy in the state begins to split open as the public believes that they no longer have a say and a voice in the government