2023-03

FRAMING THREATS TO HOMELAND SECURITY

Komzelman, Michael J.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FRAMING THREATS TO HOMELAND SECURITY

by

Michael J. Komzelman

March 2023

Thesis Advisor:	Erik J. Dahl
Second Reader:	Tristan J. Mabry

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE FRAMING THREATS TO HOMELAND SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael J. Komzelman	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

State and non-state actors like Russia and the Alt-Right use disinformation campaigns to target social and political fractures and polarize society on sensitive issues. U.S. agencies have continued to utilize variations of the same counter disinformation measures for the last 50 years. These measures have failed to keep pace with innovations by disinformation actors due to changes in the information environment and the speed of information diffusion. This thesis examines how framing theory can assist U.S. counter disinformation efforts. Framing theory proposes that the context, or frame, in which information is presented influences how individuals process the received information. In the context of this thesis, development of a strong frame consists of three elements: volume, credibility, and resonance. These elements are applied to three disinformation campaigns—Operation Denver, a Soviet campaign attributing HIV to the U.S.; #Pizzagate, a 2016 election interference campaign; and Plandemic, a non-state actor campaign targeting U.S. COVID-19 policy makers—and the countermeasures employed by U.S. agencies to each. This thesis contrasts disinformation campaigns and countermeasures using framing to demonstrate elements employed by disinformation actors and U.S. agencies to determine key differences that contribute to the successes and failures of disinformation countermeasures. This thesis proposes incorporating framing analysis into countermeasure planning and execution.

14. SUBJECT TERMS disinformation, framing theory, framing effect, Operation Denver, 2016 Election, COVID-19	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

FRAMING THREATS TO HOMELAND SECURITY

Michael J. Komzelman
Lieutenant, United States Navy
BA, California State University, San Marcos, 2013

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2023**

Approved by: Erik J. Dahl
Advisor

Tristan J. Mabry
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

State and non-state actors like Russia and the Alt-Right use disinformation campaigns to target social and political fractures and polarize society on sensitive issues. U.S. agencies have continued to utilize variations of the same counter disinformation measures for the last 50 years. These measures have failed to keep pace with innovations by disinformation actors due to changes in the information environment and the speed of information diffusion. This thesis examines how framing theory can assist U.S. counter disinformation efforts. Framing theory proposes that the context, or frame, in which information is presented influences how individuals process the received information. In the context of this thesis, development of a strong frame consists of three elements: volume, credibility, and resonance. These elements are applied to three disinformation campaigns—Operation Denver, a Soviet campaign attributing HIV to the U.S.; #Pizzagate, a 2016 election interference campaign; and Plandemic, a non-state actor campaign targeting U.S. COVID-19 policy makers—and the countermeasures employed by U.S. agencies to each. This thesis contrasts disinformation campaigns and countermeasures using framing to demonstrate elements employed by disinformation actors and U.S. agencies to determine key differences that contribute to the successes and failures of disinformation countermeasures. This thesis proposes incorporating framing analysis into countermeasure planning and execution.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIDS	Acquired Immune Deficiency Syndrome
AMWG	Active Measures Working Group
CDC	Centers for Disease Control
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus disease 2019
DCCC	Democratic Congressional Campaign Committee
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNC	Democratic National Committee
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
FBI	Federal Bureau of Investigation
GEC	Department of State's Global Engagement Center
GRU	General Staff of the Russian Army
HHS	Department of Health and Human Services
HIV	Human Immunodeficiency Virus
IRA	Internet Research Agency
KGB	Komitet Gosudarstvennoy Bezopasnosti
NIAID	National Institute of Allergy and Infectious Diseases
NSC	National Security Council
USIA	United States Information Agency

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Thank you to my loving, patient wife, Kari; my supportive parents; my sounding board, Michener; and my very patient advising team.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

Disinformation campaigns are becoming increasingly common and used to target a range of issues critical to U.S. governance. There have been campaigns during major elections, against public health campaigns such as the fight against the COVID-19 pandemic, and even against state policy issues such as immigration reform. The range of information sharing services like traditional media, and now social media, and near universal access to the internet has made the scope of these campaigns increasingly dangerous. The broad purpose of such attacks is to destabilize trust in critical institutions and undermine key institutions, including but not limited to the U.S. government, medical professionals, and law enforcement. The way these challenges are framed significantly affects public opinion and support throughout the population. Framing theory describes how these sources influence opinion and action by applying context, or the bias of the information source. This thesis asks: Can framing theory be applied to understand disinformation campaigns? And if so, what lessons can it offer to effectively counter current disinformation methods?

B. PROBLEM STATEMENT

Disinformation campaigns work by distorting the truth and creating an alternate version of events to create doubt. For example, a disinformation actor may attempt to discredit a political candidate by releasing disinformation about the candidate's dubious personal connections using altered photographs. Similarly in the medical field, a disinformation actor may undermine a healthcare facility or institution by publicly making fallacious medical malpractice claims against healthcare workers.

Disinformation defines the attempt to strategically alter perceptions through deception; comparably, studies into the framing effect attempts to identify how societies develop value narratives that give meaning to their world views. Deception and framing are the tools through which disinformation occurs. The framing effect describes how information manipulators can affect the population's opinions on issues through applying

their own context to issues. This has been the primary focus of both political science and communications studies on the framing effect.[1] These two areas of study have tremendous untapped overlapping significance. Better understanding of disinformation frames may enable innovative ways to combat disinformation.

Due to the range, complexity, and variety of disinformation campaigns, a comprehensive model for combating various disinformation campaigns has been simplified to a three-pronged model: deny, refute, riposte. The goal of this model is to deny the disinformation actor access to the information space, refute a disinformation actor's fallacious claims, and to undermine a disinformation actor's credibility to expose their disinformation efforts. The Department of Homeland Security (DHS), the U.S. State Department's Global Engagement Center (GEC), and counter disinformation antecedent the Active Measures Working Group (AMWG) have adapted varying degrees of this model.[2] However, each of these three methods has pitfalls that prevent effectiveness. First, prevention of disinformation can become a First Amendment issue when the source appears to be a U.S. citizen. Second, directly confronting the disinformation campaign does not necessarily sway the population that has become distrustful of the U.S. supported subject matter experts. Finally, attacking the disinformation source can create a backlash due to apparent targeting of that disinformation source.

---

[1] Dennis Chong and James N. Druckman, "Framing Theory," *Annual Review of Political Science* 10, no. 1 (June 1, 2007): 109, https://doi.org/10.1146/annurev.polisci.10.072805.103054.

[2] U.S. State Department Global Engagement Center, "GEC Counter-Disinformation Dispatches # 2 – Three Ways to Counter Disinformation," February 11, 2020, https://e.america.gov/t/ViewEmail/i/95383D12423453CD2540EF23F30FEDED/5069D0DCBA89C0A1EBAD456BEB5F1DD6; Department of Homeland Security, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 2019, 23, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf; Fletcher Schoen and Christopher J Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Institute for National Strategic Studies* No. 11 (June 2012): 39, 47, https://ndupress.ndu.edu/portals/68/documents/stratperspective/inss/strategic-perspectives-11.pdf. The GEC advocates three ways to counter disinformation: prevent the initial disinformation claims before they become pervasive, provide a counter information campaign to correct misperceptions, or discredit the disinformation source. Similarly, DHS recommends three themes: "hit the actor [riposte], hit the technology [deny], and build public resilience [refute]." The AMWG, predecessor to modern disinformation efforts, pioneered U.S. counter disinformation efforts; their tactics were to confront disinformation efforts with "fact-based research and publicity" in which they exposed the Soviet Union's disinformation campaigns' malicious disinformation, sources, and tactics.

C. LITERATURE REVIEW

The following section provides an analysis of existing research on disinformation campaigns, counter-efforts by U.S. agencies, and links to framing theory. First, there is an extensive analysis of the available disinformation literature: defining disinformation and addressing the structure and means utilized to spread disinformation. Second, there is an assessment of the various means employed by U.S. agencies and their partners to address the variety of disinformation approaches. Their methods have fallen into three distinct camps: limiting, countering, or discrediting the source. Third is an explanation of how adversaries and U.S. agencies compete to control the information domain and the role framing plays in that competition. The framing effect provides a conduit through which disinformation or counter measures affects the recipients, in this case U.S. citizens.

1. Disinformation

Disinformation has been a part of warfare dating back to Sun Tzu's most notable quotation: "All war is based on deception."[3] In the early twentieth century, weaponized information became more popular in a new context, targeting not only adversaries but citizens within the state as well, giving rise to a new field in social control – propaganda. Edward Bernays defined propaganda as "manipulating the social machinery which controls the opinions and habits of the masses."[4] Propaganda through the early part of the century supported the rise of regimes and altered social paradigms but now bears a more severe negative connotation.[5] In recent years, propaganda has shifted to the background while subsets such as disinformation, advertising, and public relations have become increasingly nuanced.

[3] Sun Tzu, *The Art of War*, UNESCO Collection of Representative Works. Chinese Series (London: New York, 1971), 68.

[4] Edward L. Bernays, *Propaganda* (Brooklyn, N.Y: Ig Publishing, 2005), 37.

[5] John B. Whitton, review of *Review of International Propaganda. Its Legal and Diplomatic Control*, by L. John Martin, *Harvard Law Review* 72, no. 2 (1958): 396–400, https://doi.org/10.2307/1338178.

a. Defining Disinformation

The broader study of false information constitutes a complex group of literature that has little to do with intent (e.g., profit, social control, or incitement). For example, Whaley describes a general theory of deception as "distortion of perceived reality."[6] Others have focused on the scope of dissemination, such as Vosoughi et al., who conducted a study using Twitter data between 2006 and 2017 and determined that falsehoods disseminate more quickly and further than truth.[7] Still others, like Wilson et al., and Allenby and Garreau, focus on the role narratives play in false information.[8]

Scholarship in the field of information distinguishes disinformation, misinformation, and malinformation into distinct categories. Naming conventions vary but scholars such as Bradshaw et al., Wardle and Derakhshan, and Colley et al. agree that disinformation and misinformation are false information separated by the intention of the disseminator.[9] Disinformation is information that is shared deliberately with an intent to do harm, whereas misinformation is unintentional in nature. Wardle and Derakhshan further distinguish malinformation as "genuine information [that] is shared to cause harm."[10] The caveat, described by Jack, is that "in practice, the lines separating advertising, public relations, and public diplomacy (terms often regarded as neutral) from the pejorative

---

[6] Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies* 5, no. 1 (March 1, 1982): 182, https://doi.org/10.1080/01402398208437106.

[7] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

[8] Tom Wilson, Kaitlyn Zhou, and Kate Starbird, "Assembling Strategic Narratives: Information Operations as Collaborative Work within an Online Community," *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (November 2018): 183, https://doi.org/10.1145/3274452; Brad Allenby and Joel Garreau, "Weaponized Narrative Is the New Battlespace," Defense One, January 3, 2017, https://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/.

[9] Samantha Bradshaw and Philip N Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," 2019, 15, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1209&context=scholcom; Claire Wardle, "Misinformation Has Created a New World Disorder," Scientific American, accessed May 21, 2022, https://doi.org/10.1038/scientificamerican0919-88; Thomas Paul Colley, Francesca Granelli, and Jente Althuis, "Disinformation's Societal Impact: Britain, COVID and Beyond," *Defence Strategic Communications* 8, no. 1 (July 3, 2020): 91, https://doi.org/10.30966/2018.RIGA.8.3.

[10] Wardle, "Misinformation Has Created a New World Disorder," 5.

term propaganda (which usually implies deliberate intent to manipulate or deceive) can be hard to discern."[11]

Disinformation, thus, is distinct from misinformation in that it is intentional, exploitive, involves deception, and targets social divisions. For example, Perkins describes the Soviet Union's use of four types "active measures" (the Soviet title for disinformation efforts) to manipulate both allies and adversaries: "media disinformation, forgeries, agents of influence, and front groups/organizations."[12] More recently, Mueller described the Russian efforts to influence the 2016 U.S. presidential election as "sweeping and systematic."[13] Also, Korta describes seventeen different scenarios – across a variety of different social issues including: public health, gun control, gender, racial and ethnic divides, party divisions, anti-government sentiment – in which disinformation resulted in damages to public health, increased tensions, and loss of life.[14]

b. Ways and Means

The study of disinformation has two research agendas: 1) the nature and 2) the scope of the deception involved. When considering the nature of disinformation, Whaley offers six different categories of deception: masking (hiding the truth), repackaging (disguising the truth as something else), dazzling (reducing "the certainty about the real nature of a thing"), mimicking (creating a similar thing and representing it as the real), inventing (a complete fabrication), and decoying (offering a diversion).[15] Disinformation as a tool can incorporate one or more categories of deception to engender the desired effect to manipulate the recipient into believing an alternate representation of information. The

---

[11] Caroline Jack, "Lexicon of Lies: Terms for Problematic Information" (Data & Society Research Institute, 2017), 6, https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf.

[12] Alexander M Perkins, "Soviet Active Measures Reborn for the 21st Century: What Is to Be Done?," December 2018, 28, https://calhoun.nps.edu/handle/10945/61246.

[13] Robert S. Mueller III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election Volume I and II" (U.S. Department of Justice, March 2019), 1, https://www.justice.gov/archives/sco/file/1373816/download.

[14] Samantha M Korta, "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security," March 2018, 1–21, https://calhoun.nps.edu/bitstream/handle/10945/58322/18Mar_Korta_Samantha.pdf?sequence=1&isAllowed=y.

[15] Whaley, "Toward a General Theory of Deception," 182–85.

second consideration is of the scope of dissemination. As demonstrated by Arif et al., social media has rapidly altered the speed at which misinformation spreads; the speed at which rumors spread online is affected by volume of content, initial exposure population size, and derived content.[16]

A final issue studied by scholars of disinformation is sourcing: where does the disinformation come from? Disinformation's intentional propagation paths are innumerable and make tracking, prevention, and countering the disinformation difficult. Donovan and Friedberg, for example, describe a process called "source hacking" in which disinformation propagators target news media and journalists, providing false information to be mixed in during breaking stories, polluting the information that would be released, causing disinformation to appear as reputable information without direct interfacing between propagators and the public.[17]

Jack describes how flooding public forums can alter public opinion, manipulate similar voices, and silence dissent.[18] The cyber domain creates both a new medium and new methods of exploitation. According to Bayer et al. these new methods include "social bots, artificial intelligence (AI), micro-targeting or paid human 'trolls.'"[19] Disinformation can now be not only outsourced but automated, and recipients can be wholly unaware and even assist in helping it spread and, by extension, increasing its credibility.

2. Theory of Countering Disinformation

In contrast to the numerous forms of disinformation campaigns, countering disinformation has fallen into only three categories: limiting the spread of disinformation

[16] Ahmer Arif et al., "How Information Snowballs: Exploring the Role of Exposure in Online Rumor Propagation," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16 (New York, NY, USA: Association for Computing Machinery, 2016), 474, https://doi.org/10.1145/2818048.2819964.

[17] Joan Donovan and Brian Friedberg, "Source Hacking," 2, accessed May 21, 2022, https://datasociety.net/wp-content/uploads/2019/09/Source-Hacking_Hi-res.pdf.

[18] Jack, "Lexicon of Lies: Terms for Problematic Information," 9.

[19] Judit Bayer et al., "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, February 1, 2019), 9, https://doi.org/10.2139/ssrn.3409279.

by targeting sources (deny), countering disinformation by providing the correct information (refute), and discrediting the source in the case that it cannot be limited (riposte). These methods are far more direct and limited when compared to the array of deceptive methods employed in disinformation campaigns.

a. Not So Free Speech

Frequently, the first approach of limiting sources of disinformation by denial is either one that occurs too little too late, or which infringes on civil liberties. The Department of Homeland Security (DHS) acknowledges that most often the ability to remove sources of disinformation is often only "post-mortem" or after the event and after security professionals cross check information determining a malicious source and informing social media providers.[20] Removing false information or fake accounts can only occur once the information or account is determined to be false. At that point, the disinformation campaign has already achieved some measure of success. West notes that "in a situation of false information, it is tempting for legal authorities to deal with offensive content and false news by forbidding or regulating it…[but] this will restrict global freedom of expression and generate hostility to democratic governance."[21] Democracies, particularly the U.S., are sensitive to this type of regulatory practice. Governments are not the only ones affected; Starbird et al. argue that social media platforms are reluctant to counter disinformation campaigns by blocking accounts due to commitment to perceived values like "freedom of speech," as well as attempted provision of "platform goals such as providing a place for activists (including those in oppressed groups) to congregate and organize."[22] Both government and industry professionals are reluctant to consider this as a practical form of countering disinformation as, in practice, it runs counter to their mission statements.

---

[20] Department of Homeland Security, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 5.

[21] Darrell M. West, "How to Combat Fake News and Disinformation," *Brookings* (blog), December 18, 2017, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

[22] Kate Starbird, Ahmer Arif, and Tom Wilson, "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations," *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 7, 2019): 19, https://doi.org/10.1145/3359229.

b. Appeal to Authority

The second method of countering disinformation (refute) requires a trusted agent to counter the false claim and present the truth; this method is heavily reliant on trust. The U.S. State Department's GEC acknowledges that in order to combat disinformation directly an expert spokesperson is required, utilizing a subject matter expert to counter false claims;[23] however, DHS asserts that disinformation campaigns are designed to undermine trust in subject matter experts.[24] If disinformation campaigns erode the trust of citizens in U.S. institutions and experts, then the claims made by the institutions and experts can no longer effectively counter campaigns against them.

There is an alternative to promoting a counter disinformation narrative from a trusted source: fighting volume with volume, filling the information space with noise in a similar fashion as disinformation distributors. The Department of State's GEC celebrated a particularly nuanced counter disinformation campaign in Lithuania, which involved scraping web pages using AI and employing "elves," "volunteers who fight pro-Kremlin 'trolls' on the internet."[25] The Lithuanians directly combatted the narratives utilized by their adversary, Russia, through this hybrid method with a state-sponsored grass-roots movement. This tactic created a cacophony in the information space to muddy the waters, but this tactic has not been adopted by either the GEC or DHS.[26]

c. Ad Hominem

The final approach is to directly discredit the source of disinformation, undermining its brand (riposte). For example, a semi-successful method utilized by the British

[23] U.S. State Department Global Engagement Center, "GEC Counter-Disinformation Dispatches # 2 – Three Ways to Counter Disinformation."

[24] Department of Homeland Security, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 6–7.

[25] U.S. State Department Global Engagement Center, "GEC Counter-Disinformation Dispatches # 1 – A Counter-Disinformation System That Works," January 8, 2020, https://e.america.gov/t/ViewEmail/i/9146D16121A6D6562540EF23F30FEDED/981423FE1274E8AFBA4AF9908B8D85ED.

[26] U.S. State Department Global Engagement Center, "GEC Counter-Disinformation Dispatches # 2 – Three Ways to Counter Disinformation"; Department of Homeland Security, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 21–25.

government (in a case study highlighted by the GEC) was to ignore the individual narratives produced in the disinformation campaign and instead expose the adversaries attempting to influence.[27] This approach can be especially successful when targeting adversarial state-run institutions, as the connection between the institution and the state is clear. These connections are especially clear with media outlets such as *RT (*formerly *Russia Today)* and *Sputnik*.[28] However, when considering alternate dissemination methods such as trolls, bots, and source hacking the source is disguised, inhibiting undermining the credibility of the source due to the intermediary proxies.

Another way to attack the source is indirectly; by changing the recipient to an unintended audience that will respond negatively to the disinformation campaign and incite a public outcry. The GEC highlighted this tactic, called "crossing their channels," which exposes propaganda to groups other than the target audience to turn the unintended audience against both the propaganda and source.[29] This form of source discreditation manipulates a third party to decry the message and source. This approach is not as successful along American social fault lines as these disinformation campaigns target internal divisions rather than external divisions when compared to the Russian/Eastern Europe social case.

3. Framing Theory

Framing theory is the story of competing narratives, much as the competition between disinformation and counter disinformation involves back and forth exchanges of different stories or narratives. Chong and Druckman state that framing theory addresses how "(often small) changes in the presentation of an issue or an event produce (sometimes

[27] U.S. State Department Global Engagement Center, "GEC Counter-Disinformation Dispatches # 2 – Three Ways to Counter Disinformation"; Alex Aiken, "RESIST 2 Counter-Disinformation Toolkit," *Government Communication Service*, 2021, 49, https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf.

[28] U.S. State Department Global Engagement Center, "Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem," January 2022, 33, https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf.

[29] U.S. State Department Global Engagement Center, "GEC Counter-Disinformation Dispatches # 2 – Three Ways to Counter Disinformation."

large) changes of opinion."[30] Not all disinformation campaigns are consistent or have plausible arguments.[31] However, the fundamental struggle between disinformation and counter disinformation campaigns is a struggle to control the narrative that informs the values of target audiences.

a. Defining the Overlap

Framing research and disinformation research are not all that different. However, framing research focuses on how narratives impact recipients, while disinformation research focuses primarily on the deceptive nature of the narrative. According to Chong and Druckman, "framing refers to the process by which people develop a particular conceptualization of an issue or reorient their thinking about an issue."[32] In disinformation literature, Canan and Akila have found that disinformation campaigns seek to alter frames (schema); while Daniel and Herbig denote this process occurs through creating an alternate narrative.[33] Tanker writes "much of the power of framing comes from the ability to define the terms of a debate without the audience realizing it is taking place."[34] Disinformation research focuses on how deception and disinformation negatively affect public values while framing studies compliment disinformation research discussing the broader competition between narratives that shape social values.

b. Competitive Framework

An area lacking in disinformation research but present in framing is the concept of *strong frame*. Disinformation and counter disinformation campaigns are defined by their

---

[30] Chong and Druckman, "Framing Theory," 104.

[31] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security" (RAND Corporation, April 27, 2017), https://www.rand.org/pubs/testimonies/CT473.html.

[32] Chong and Druckman, "Framing Theory," 104.

[33] Mustafa Canan and Anthony Akil, "A Warfare Domain Approach to the Disinformation Problem," March 2020, 83, https://www.proquest.com/openview/0b9049cf147a8a355400012a72755a4a/1?pq-origsite=gscholar&cbl=396500; Donald C. Daniel and Katherine L. Herbig, "Propositions on Military Deception," *Journal of Strategic Studies* 5, no. 1 (March 1, 1982): 155–77, https://doi.org/10.1080/01402398208437105.

[34] James W. Tankard Jr., "Chapter 4: The Empirical Approach to the Study of Media Framing," in *Framing Public Life: Perspectives on Media and Our Understanding of the Social World*, ed. Stephen D. Reese, Oscar H. Gandy Jr, and August E. Grant (Routledge, 2001), 97.

end results rather than the process of what makes a frame more or less appealing. Chong and Druckman theorize that there are three components that affect a frame's strength: volume, credibility, and resonance.[35] The more frequently an individual hears information and the more sources they hear it from, the more likely it is that the information becomes part of their schema. The credibility of the source also matters, whether on a personal or professional level; a trusted friend's perspective or a subject matter expert can alter how individuals develop their personal frames. Resonance refers to how closely a frame is congruent with an already existing world view; Sniderman and Theriault conclude that while comparing contrasting frames, individuals are more likely to accept the frame that is consistent with their world view.[36]

Competing frames are comprised of a struggle of narratives. Wilson et al. note that "narratives allow humans to structure information, giving meaning to actions that facilitate sensemaking."[37] Repeated, overlapping narratives form the basis for frames. Erbschloe argues that these indirect changes are not necessarily noticeable and may contribute to the creation of cognitive biases.[38] When this process is coupled with dissimilar narratives, each individual's schema or collection of frames begin to differ from one individual to the next These subtle deviations, over time, form the basis for ideological camps that rally; seeking information that resonates with their collective world view. According to Canon and Akil, repetitive exposure to narratives that resonate with individuals make them more susceptible to further information (i.e., programming).[39] This process allows even like-minded individuals to alter their perspectives over time, forming entirely different frames through which they perceive the world.

---

[35] Dennis Chong and James N. Druckman, "A Theory of Framing and Opinion Formation in Competitive Elite Environments," *Journal of Communication* 57, no. 1 (2007): 104, https://doi.org/10.1111/j.1460-2466.2006.00331.x.

[36] Paul M. Sniderman and Sean M. Theriault, "Chapter 5 The Structure of Political Argument and the Logic of Issue Framing," in *Studies in Public Opinion: Attitudes, Nonattitudes, Measurement Error, and Change* (Princeton University Press, 2004), 133–65, https://doi.org/10.2307/j.ctv346px8.

[37] Wilson, Zhou, and Starbird, "Assembling Strategic Narratives," 183:4.

[38] Michael Erbschloe, *Extremist Propaganda in Social Media: A Threat to Homeland Security* (Boca Raton, FL: CRC Press, Taylor & Francis Group, 2019).

[39] Canan and Akil, "A Warfare Domain Approach to the Disinformation Problem," 83.

c. Limitations

The incredible range and omnipresence of framing as a concept makes it difficult to isolate and study. Performing research on framing most often focuses on a case study approach or attempts to determine if causal factors can be isolated in a meaningful way.[40] Attempting to identify a single independent variable as a causal factor among multiple influencing factors about a specific issue is vexing; further, dependent variables interact and influence each other to the extent that they are inextricably linked.[41]

D. POTENTIAL EXPLANATIONS AND HYPOTHESIS

Two possible efforts can increase the efficacy of U.S. agency counter measure efforts. Current counter disinformation efforts follow a static application of the deny, refute, riposte model while innovations in technology, communication, and digital social interaction volume outpace the employment of the model. Employment of the current model to combat a litany of disinformation campaigns simultaneously in the current information environment is both cost ineffective and time inefficient; the model, however, is not without merit and can be improved.[42] Incorporation of framing may increase the efficacy of countermeasures. Rather than attempting to counter disinformation directly, framing concepts may better assist countermeasure efforts through better focus of countermeasure through targeting frames or undermine aspects of frames generated in disinformation actors' campaigns. This section describes two hypotheses for strategies that may improve the effectiveness of U.S. counter disinformation strategies.

---

[40] Francesca Polletta and M. Kai Ho, "Frames and Their Consequences," in *The Oxford Handbook of Contextual Political Analysis*, 2006, 16, https://doi.org/10.1093/oxfordhb/9780199270439.003.0010.

[41] James N. Druckman, "The Implications of Framing Effects for Citizen Competence," *Political Behavior* 23, no. 3 (2001): 236–37, https://doi.org/10.1023/A:1015006907312; Donald P. Haider-Markel and Mark R. Joslyn, "Gun Policy, Opinion, Tragedy, and Blame Attribution: The Conditional Influence of Issue Frames," *The Journal of Politics* 63, no. 2 (2008): 522, https://doi.org/10.1111/0022-3816.00077; David C. Barker, "Values, Frames, and Persuasion in Presidential Nomination Campaigns," *Political Behavior* 27, no. 4 (2005): 378, https://doi.org/10.1007/s11109-005-8145-4.

[42] Department of Homeland Security, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 21–23.

Hypothesis One: More effective counter disinformation strategies can undermine disinformation campaigns by only disseminating factual information and not targeting the disinformation narrative.

This hypothesis attempts to disarm disinformation campaigns by targeting specific components of an adversary's frame or narrative. This hypothesis postulates that rather than targeting disinformation campaign narratives, a better strategy would focus on only building a strong narrative using the factual information. For example, a disinformation campaign targeting the American public health sector associates the origin of a tenacious infection with questionable government activity in Missouri; however, the origin of the infection is a microbe in processed meat. Rather than attempting to deny the claimed association, a countermeasure campaign should run against the origin of the infection, while disregarding the attempted association with the government activity.

Hypothesis Two: Countermeasures can be improved, and efficacy increased, by applying concepts of a strong frame (volume, credibility, and resonance).

This hypothesis posits that counter disinformation operations can be improved by using the three concepts of a strong frame: increasing dissemination to increase viewership and interaction, using a range of credible sources to bolster each other and cement credibility, and improve public reaction by shaping the frame in a way that is more agreeable to target audiences. For example, a disinformation actor seeks to exploit an opportunity created due to a controversial bit of legislation up for a vote in a coming voting cycle by connecting the legislation to social divisions like race, gender, and party affiliation. According to the second hypothesis, a counter disinformation campaign would attempt to increase dissemination of factual information to dominate the disinformation in the information sphere, leverage the credibility of bipartisan experts to undermine the disinformation, and be geared toward and engage with susceptible populations.

E. RESEARCH DESIGN

This thesis analyzes current practices in countering disinformation campaigns through multiple case studies. The three case studies selected range in scope to depict a

range of disinformation campaigns: one historical state sponsored case, one divergent state sponsored case, and one non-state actor case.

Disinformation attacks against the U.S. seek to undermine democratic values, reduce faith in institutions, and incite social panic or outrage. The case studies were chosen to include a sample case including each desired effect. Election tampering or interference in government institutions erodes public trust.[43] Medical disinformation campaigns deteriorate public health, can exacerbate infection and transmission rates, and degrade faith in trusted experts.[44] In times of crisis, such as pandemics, citizens are on edge and more susceptible to disinformation attacks prompting more extreme reactions. Specific case studies are outlined in the chapter overview below.

Materials used in establishing the sequence of events and government responses are all unclassified documents, accounts, reports, press releases, and when possible, source material of social media posts. Numerous documents, reports, and press releases document the sequence of events and responses to specific campaigns such as the *Homeland Security Affairs Journal: SPECIAL COVID-19 ISSUE* or the Senate Select Committee on Intelligence's *Russian Active Measures Campaigns and Interference in the 2016 U. S. Election*. Compiled analysis research such as *Network Propaganda* details the chronology of events, providing both sourcing and primary frame development insights that were invaluable.

These sources provided extensive material used to construct primary, secondary, and follow-on frames for comparative analysis. This line of research establishes a core narrative and provides insights into the web of disinformation frames used by adversaries. Patterns indicate vulnerabilities in disinformation frames that could be exploited by counter disinformation professionals. Comparisons between disinformation and counter disinformation frames identify best practices that present opportunities for improvement.

[43] U.S. State Department Global Engagement Center, "Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem," 17.

[44] Wesley R Moy and Kacper Gradon, "COVID-19 Effects and Russian Disinformation Campaigns," no. 2020 (2020): 4, 9, https://www.hsaj.org/articles/16533.

F. CHAPTER OVERVIEW

This thesis will include five chapters. The introduction will set the stage for the following case study sections. Chapter II examines Operation Denver, a historical case study with a state actor propagating disinformation. Chapter III examines #Pizzagate, one of the many disinformation campaigns during the 2016 election, and the postmortem findings of the U.S. Senate and private partner investigations. Chapter IV examines *Plandemic*, a non-state actor campaign conducted at the height of COVID-19. Each chapter outlines a disinformation campaign and analyzes frame development of the disinformation campaign followed by the counter disinformation campaign, analysis of the countermeasures, and hypothesis application. Chapter V synthesizes the findings throughout Chapters II-IV on the three aspects of a strong frame (volume, credibility, and resonance), makes recommendations, and identifies areas for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. OPERATION DENVER

A. INTRODUCTION

This chapter examines a Soviet medical disinformation campaign, and the tactics employed to counter it by U.S. agencies, and then analyzes each by applying Framing Theory. The chapter will first outline a historical perspective of the campaign followed by an examination of the capacity of the campaign to alter a target's world view or—to use framing terminology—schema. The examination of the disinformation campaign will include the types of deception and strong frame concepts previously examined in Chapter I. Next, this chapter will outline the countermeasures employed to counter the disinformation campaign and the countermeasures' schema. Similarly, the strong frame concept and hypotheses will be applied to the countermeasures to identify how effective the counter disinformation campaign was at generating a strong frame and identify any shortfalls.

This case, known as Operation Denver, was selected for three reasons: its historical significance and perspective, its infamy, and its straightforward framework. Occurring in the 1980s, abundant literature indicates Operation Denver was a disinformation campaign brought on by the simmering conflict between the U.S. and the USSR with enduring echoes that still affect targeted populations. The campaign itself demonstrates a clear-cut progression from correct information to an alternate disinformation framework, building on itself internally and expanding outward, making it an appropriate case for the application of Framing Theory. The countermeasures employed by U.S. government agencies are the standard three-part model discussed in Chapter I—deny, refute, riposte—allowing for direct analysis and assessing if hypothesis one (focusing on dissemination of correct information effectively counters disinformation) and two (building a strong frame to counter disinformation) can improve countermeasures.

B. DISINFORMATION CAMPAIGN

Operation "Denver" or as it is more commonly known Operation *Infektion* was a coordinated disinformation campaign to attribute the outbreak of the human

immunodeficiency virus (HIV) that leads to Acquired Immune Deficiency Syndrome (AIDS) to fallacious U.S. biological weapons experiments.[45] The AIDS epidemic created the opportunity for one of the most sensationalized disinformation campaigns ever. The premise was simple: the U.S. secretly developed HIV and their experiments "spun out of control."[46] The campaign, however, was extraordinarily complex, spanning half a decade and sporadically appearing from seemingly unconnected sources despite one singular source—the Soviet Union.

The first iteration of the connection between AIDS and the U.S. government was in 1983 in the New Delhi *Patriot* magazine.[47] Patriot's purported source: an anonymous '"well-known American scientist and anthropologist"' who implicated the Pentagon, U.S. Army Fort Detrick, and "scientists from the Centers for Disease Control (CDC) in Atlanta, Georgia."[48] Two years later, the story was then picked up by Soviet media sources first in *Literaturnaya Gazeta* and then circulated widely through Soviet media satellites throughout the developing world who had little ability, or possibly incentive, to fact check developing stories.[49] In parallel, a 52-page quasi-scientific report was produced, and cited in later versions of the disseminated articles, by an East German scientist, Professor Jacob

[45] Douglas Selvage and Christopher Nehring, "Operation 'Denver': KGB and Stasi Disinformation Regarding AIDS | Wilson Center," *Operation "Denver": KGB and Stasi Disinformation Regarding AIDS* (blog), July 22, 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids.

[46] Douglas Selvage, trans., "KGB, Information Nr. 2955 [to Bulgarian State Security]" (Wilson Center Digital Archive, Committee for Disclosing the Documents and Announcing the Affiliation of Bulgarian Citizens to the State Security and the Intelligence Services of the Bulgarian National Army (CDDAABCSSISBNA-R), September 7, 1985), 1, f. 9, op. 4, a.e. 663, https://digitalarchive.wilsoncenter.org/document/102957/download.

[47] Elad Simchayoff, "Operation Infektion," *Lessons from History* (blog), July 30, 2020, https://medium.com/lessons-from-history/operation-infektion-a1485fe85443.

[48] United States Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87," August 1987, 34, https://books.google.com/books?hl=en&lr=&id=JaZv3QJCdKMC&oi=fnd&pg=PR8&dq=%22Soviet+Influence+Activities:+A+Report+on+Active+Measures+and+Propaganda,+1986+-+87%22&ots=RF-Z_m6duF&sig=hAYCl9vu8bmhVHBWOjgaS02QcLc#v=onepage&q=%22Soviet%20Influence%20Activities%3A%20A%20Report%20on%20Active%20Measures%20and%20Propaganda%2C%201986%20-%2087%22&f=false.

[49] United States Department of State, 34, 38.

Segal, in 1986 hypothesizing HIV's synthesized origins based on '"assumptions" and a "chain of circumstantial evidence."[50]

By 1987, the campaign reached the American public. On the CBS Evening News on March 30, Dan Rather reported to 15 million American viewers the claims that proliferated under Soviet direction. He stated that the Soviet Union claims HIV was "leaked from a U.S. Army laboratory conducting experiments in biological warfare" and, despite lack of evidence, "claims to be reporting the conclusions of unnamed scientists in the United States, Britain and East Germany."[51]

1. The Campaign in Frame

This campaign is straightforward, for the most part following a singular narrative thread, namely blaming the creation of HIV on the U.S. government with just enough factual information to make the campaign seem plausible. The campaign mixes Whaley's repackaging and inventing categories of deception to blend U.S. research and U.S. military locations into a fabrication linking the U.S. government to the AIDS outbreak.[52] Using multiple, seemingly independent sources, the campaign self-corroborated from its starting point in the "Patriot" article creating a deluge of articles in line with Jack's description of flooding public forums to alter public perception.[53]

Later efforts by the KGB, in coordination with the Stasi, the East German Ministry of State Security, sought to further alter the created schema, creating secondary and tertiary narratives. These were divided along racial lines with purported illegal biological weapons experimentation providing the basis of the original disinformation.[54] The campaign, as a

[50] United States Department of State, 35.

[51] Robert Gillette, "AIDS: A Global Assessment : Soviets Suggest Experiment Leaks in U.S. Created the AIDS Epidemic," *Los Angeles Times*, August 9, 1987, https://www.latimes.com/archives/la-xpm-1987-08-09-ss-592-story.html.

[52] Whaley, "Toward a General Theory of Deception," 182.

[53] Jack, "Lexicon of Lies: Terms for Problematic Information," 9.

[54] Selvage and Nehring, "Operation 'Denver,'" 51–57. The KGB's narrative targeted African Americans and minority groups claiming that AIDS was a measure of U.S. government social control to designed reduce unwanted populations.

whole, resembled a house of cards folding in on one original document at its center. A chronological representation of the disinformation narrative appears in Figure 1.

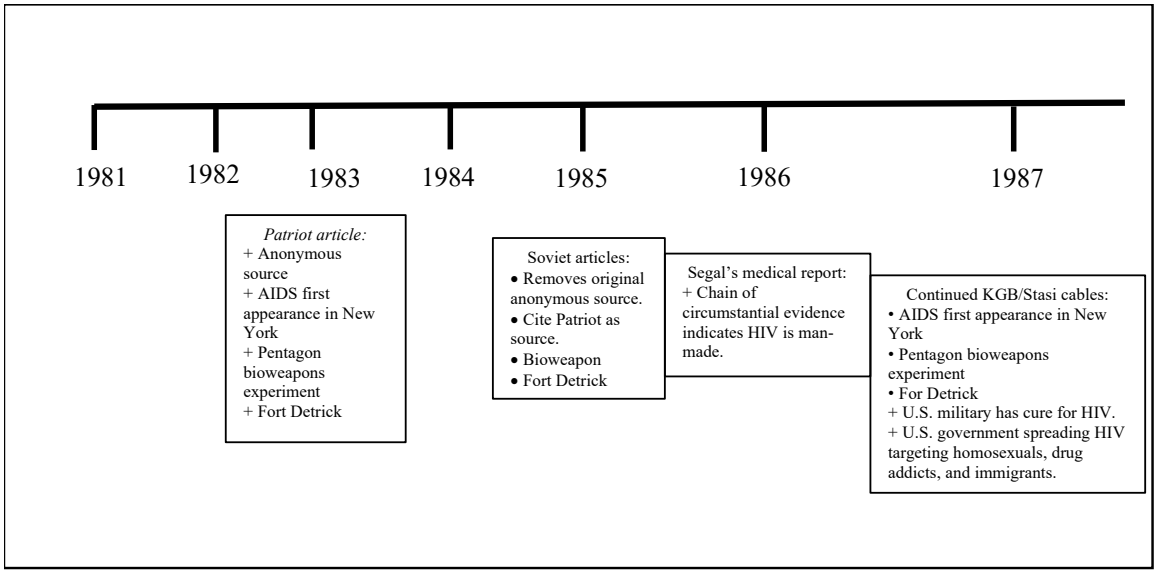


Figure 1. Disinformation campaign timeline.[55]

An analysis of the strength of the frame indicates the campaign was remarkably successful in taking up space in the information environment (volume), markedly successful in generating trustworthiness in "reputable sources" (credibility), and ambiguously successful in resonating with the target audiences' world view (resonance). The dissemination of the campaign reached a global scale, especially in areas with little access to up-to-date information.[56] The campaign itself entirely lacked credibility; however, the way in which it layered original sources, hiding the originally weak sources, resulted in media attention or "source hacking" (described by Donovan and Friedberg) of one of America's most prominent journalists: Dan Rather.[57] Rather's report, picked up by

[55] Adapted from United States Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87," 34, 38; Selvage and Nehring, "Operation 'Denver.'"

[56] United States Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87," 38.

[57] Donovan and Friedberg, "Source Hacking." Source hacking is the process of manipulating a credible source, in this case Dan Rather, into reporting disinformation as information, leveraging their credibility.

other journalists and influencing segments of society, swayed unknowing participants in the spread of the campaign.

The resonance of the campaign with some intended target audiences can still be felt to this day. For example, continued disinformation narratives propagated by the KGB/Stasi instigated racial connections which remain ingrained in minority populations like African Americans. In 2005, Bogart and Thorburn found that almost 50 percent of their sample African American population still believed AIDS was manmade and that more than 16 percent believed AIDS was a form of government control.[58] Through expeditious dissemination, hijacking of credibility of influential journalists, and exceptional resonance with disenfranchised audiences, Operation Denver successfully generated a strong enough frame to remain resonant to this day.

2. Counter-Disinformation Campaign

Primary counter-disinformation efforts were developed by a part-time intelligence collective called the Active Measures Working Group (AMWG). Spearheaded by the U.S. State Department, the group was created in 1981, just a few years before Operation DENVER began. It followed a realignment of intelligence community priorities under Ronald Reagan to dedicate more effort to identifying and countering subversion and propaganda.[59] The State Department chaired the group with members from the CIA, FBI, DOD, United States Information Agency (USIA), and later DIA and even NSC staff.[60] Their strategy was to centralize reports of disinformation, correlate and analyze the disinformation, and confront it "with fact-based research and publicity."[61] Throughout their tenure, the AMWG released Foreign Affairs Notes and reports in addition to informing foreign intelligence services and journalists of their susceptibility to

[58] Laura M. Bogart and Sheryl Thorburn, "Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention Among African Americans?," *JAIDS Journal of Acquired Immune Deficiency Syndromes* 38, no. 2 (February 1, 2005): 213, https://journals.lww.com/jaids/fulltext/2005/02010/are_hiv_aids_conspiracy_beliefs_a_barrier_to_hiv.14.aspx.

[59] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 26.

[60] Schoen and Lamb, 35.

[61] Schoen and Lamb, 39.

disinformation propagation through presentation of the intricate details and falsehoods in active disinformation campaigns.[62] These products served to increase understanding and awareness of disinformation, and attempted to help inhibit the spread of disinformation; however, due to the lack of broader readership the results were minimally effective.

Although their products had value overall, the AMWG's fact-based approach to the Soviet AIDS disinformation campaign initially had minimal results. The effect became notable not due to their tried-and-true method but due to an entirely unexpected event. In July of 1987, the AMWG released a Foreign Affairs Note titled "The U.S.S.R.'s AIDS Disinformation Campaign" detailing: the incongruities of the campaign (*Patriot*'s dubious connections, Segal's questionable report, and consistency with other Soviet claims); factual scientific data surrounding HIV; and the U.S. measures taken to counter the campaign including political letters of protest, public engagement throughout the world, and direct political discourse.[63] Following the note's initial release, The AMWG produced the comprehensive report *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–1987* detailing the AMWG's findings on all Soviet disinformation campaigns that year.[64] It was this report that achieved prominence as a result of a very public dispute. On October 27, 1987, at a well-attended U.S.-Soviet Summit, then U.S. Secretary of State George P. Schultz fired back at the Soviet leader Mikhail Gorbachev's loud complaints (about the contents of the *Soviet Influence Activities* report) stating "the lies the Soviets were spreading about AIDS were 'bum dope.'"[65] This very public altercation between Shultz and Gorbachev popularized the report and resulted in Gorbachev's public acknowledgement of the campaign days later. This dispute is widely

[62] Schoen and Lamb, 40–53. Foreign Affairs Notes are documents, smaller than reports, generated on a singular topic and disseminated to increase understanding on a particular topic – in this case, the influence operations surrounding AIDS.

[63] United States Department of State, "Foreign Affairs Note: The U.S.S.R.'s AIDS Disinformation Campaign" (U.S. Department of State, July 1987), https://books.google.com/books?id=kWhpAAAAMAAJ&pg=PA4&source=gbs_selected_pages&cad=2#v=onepage&q&f=false.

[64] United States Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87."

[65] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 6.

considered a turning point, after which the HIV disinformation campaign was no longer sponsored by the Soviet Union's political leadership. However, the KGB and fringe Soviet elements continued to expand their disinformation campaign, targeting the U.S. military, citing biological weapons development, targeted use on African Americans, and linking the African origin theory to racism.[66] Soviet leadership distanced themselves from the continuation of the campaign.[67]

The counter-disinformation campaign was a mixed success. When the U.N. General Assembly declared HIV to be a naturally occurring retrovirus, the scientific community, including the Soviet Union, and the political sphere concurred.[68] However, the AMWG's work did not prevent Dan Rather from repeating Soviet disinformation. Following his report, an AMWG member lamented '"unfortunately, nothing we can do or say will have the impact of a Dan Rather on the evening news."'[69] In other areas, some of the social consequences that slipped past counter-disinformation efforts resulted in an enduring disinformation legacy of HIV tied to targeting by race.

3. The Counter-Campaign Framed

The AMWG's efforts are a clear-cut representation of the deny, refute, riposte model of counter disinformation. The AMWG attempted to deny access to a larger audience through AMWG led training presentations to unwitting journalists and foreign intelligence services. They used fact-based research to refute the Operation Denver falsehood that HIV was manmade. Their reports consistently named the Soviet Union as the source of the disinformation. But the effectiveness of their counter disinformation campaign was not due to their hard work and dedication but from a coincidence that highlighted their efforts. The inability to reach a target audience, media intermediaries, is

[66] African origin theory is the accepted theory positing transition from Simian Immunodeficiency Virus (SIV) to HIV through ingestion of contaminated meat originating in Africa.

[67] Douglas Selvage, "Operation 'Denver': The East German Ministry for State Security and the KGB's AIDS Disinformation Campaign, 1986–1989 (Part 2)," *Journal of Cold War Studies* 23, no. 3 (2021): 14, 16–19, 45–52, https://muse.jhu.edu/pub/6/article/801905.

[68] Selvage, 14–16.

[69] Gillette, "AIDS: A Global Assessment : Soviets Suggest Experiment Leaks in U.S. Created the AIDS Epidemic."

illustrated by the failure to prevent even prominent American journalists from spreading disinformation about HIV. The limitations of their counter disinformation measures are apparent: limited ability to deny disinformation access to the information sphere and limited scope of readership.

The AMWG's counter disinformation campaign took the opposite approach of the first hypothesis, targeting of only the false information, with the preponderance of their counter disinformation efforts. The AMWG's primary counter effort was providing facts belying the credibility of fallacious claims and showing the disinformation trail led back to the Soviets. There was little emphasis on the kernels of truth embedded in the disinformation campaign. The AMWG's Foreign Affairs Note *The U.S.S.R.'s AIDS Disinformation Campaign* deconstructs the narrative created by the disinformation campaign rigorously through the first 9 pages of the 14 page document. However, it then lists facts in abundance among sundry annexes of counter information addressing HIV, U.S. institutions, and a chronological accounting of international appearances of AIDS related disinformation.[70] The major effort of the AMWG was to disentangle the narrative, which is the opposite of the premise of the hypothesis. The information they provided in the annexes contained complex jargon like explanations of lentiviruses, oncogenic retroviruses, and tentiviruses—completely inaccessible to the lay person.[71] The inaccessibility of their factual evidence provides little support for this hypothesis. This case does not support hypothesis one.

This case supports hypothesis two, by incorporating concepts from Framing theory—in particular the concepts of a strong frame (volume, credibility, and resonance)—disinformation countermeasures effectiveness can be improved. The AMWG's counter disinformation efforts lacked critical components of a strong frame. Although the AMWG's primary purpose was countering Soviet disinformation campaigns, and they produced documents and provided information to increase resistance to disinformation

[70] United States Department of State, "Foreign Affairs Note: The U.S.S.R.'s AIDS Disinformation Campaign," 10–14.

[71] United States Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87," 44.

campaigns, they simply lacked the media presence necessary to prevent the spread of disinformation. Their efforts were muted until the explosive exchange between Shultz and Gorbachev which was little attributed to the AMWG. The AMWG relied on their impeccable credibility. Early in AMWG's endeavors, prior to Operation Denver, the team learned that unless their information was beyond reproach, their counter disinformation efforts could be countered by Soviet officials; therefore, the information used to counter this campaign was impeccable, and traceable to the smallest detail.[72] The AMWG's ability to resonate with the U.S. population was limited by the scope of their disseminated articles, reports, and briefs—mainly targeting information intermediaries such as media outlets and cooperative foreign intelligence services rather than the general public. This means that the majority of their efforts were toward preventing dissemination rather than refuting disinformation already spread. In sum, the AMWG was successfully credible, on paper, but lacked voice in the public sphere (volume) and sought to guide the wrong target audience (resonance).

The strength of their frame could be increased in both volume and resonance. Increasing viewership and public engagement while leveraging their rock-solid credibility may have increased their ability to counter Operation Denver. Even more thorough engagement with the press may have prevented the story from being broadcast by Dan Rather. Second, increasing resonance with the general population, including disenfranchised (at risk) populations, was not part of the AMWG's counter disinformation campaign. As a result, target groups remain affected by the disinformation campaign.

C. CONCLUSION

Operation Denver depicts a significant near-modern disinformation campaign, coordinated by a state, the U.S.S.R., with significant resources targeting another state, the U.S. Although the information environment is significantly different today, this case provides significant insights into the structure and frames of disinformation campaigns. In the framing context, Operation Denver utilized dissimilar sources to flood the information

[72] Schoen and Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 43.

sphere and adapt to the information environment, "hacked" scientists and journalists to increase credibility, and targeted disenfranchised populations to significant effect.

In contrast, the U.S. government response, the AMWG, demonstrated critical deficiencies. The AMWG operated only part-time, indicating a lack of dedicated resources. Their reports and presentations provided inscrutable evidence of disinformation operations but suffered from both a lack of readership and influence on their own target audience—press and intelligence services. Their products provided little to the general public. In this way, the AMWG relied on one aspect of a strong frame, credibility, but was unable to generate readership (volume) prior to the Schultz-Gorbachev altercation and influence among target populations (resonance). Even with the substantial boost in publicity from Schultz and Gorbachev's exchange, target populations remain affected by this near 60-year-old campaign.

The counter disinformation campaign suffered critical flaws when compared to the disinformation campaign. Operation Denver created a strong frame; in contrast, the AMWG only developed one aspect of a strong frame. Resources, time and effort, may have increased the effectiveness of countermeasures indirectly. However, without reaching target populations and tailoring content to those audiences, the effects of increased resources will be muted. Hypothesis one predicted that by providing factual information (instead of countering the constructed narrative) the disinformation campaign will naturally be dismissed; the AMWG provided both a deconstructed narrative and factual information, but both were weakened by the initial obscurity of the report, reaffirming the necessity of both increased dissemination (volume) to the targets of disinformation (resonance).This supports hypothesis two—building a strong frame can increase countermeasure efficacy.

III. 2016 ELECTION

A. INTRODUCTION

This chapter will apply framing concepts to one politically motivated disinformation campaign: #Pizzagate. First, it is necessary to examine two critical precursor events in 2016 to establish the threads necessary for its conception. Next, the #Pizzagate campaign will be outlined followed by framing contextual analysis. In contrast to other cases, the next section examines postmortem Congressional findings of collective disinformation efforts surrounding a greater number of campaigns of which #Pizzagate is only one. And finally, hypothesis one (targeting only the false information) and hypothesis two (building a strong frame to counter disinformation) will be applied to the troubling findings of the reports.

There are numerous reasons to select a campaign that occurred during the 2016 U.S. Presidential election, including the effects of disinformation campaigns on events with significant national security implications. Secondly, the politically charged environment lends itself particularly well to the spread of disinformation. Thirdly, the information cycle is particularly condensed with 24-hour news coverage of various issues. #Pizzagate in particular was selected due to two factors: the speed of inception and the violent conclusion. The #Pizzagate campaign highlights problematic elements of the deny, refute, riposte counter disinformation model due to the apparently innocuous starting point of the campaign, its explosive growth, and violent conclusion.

B. #PIZZAGATE

What do you get when you combine Russian hackers, internet trolls, dubious journalists, and a willing audience? In late 2016, the answer was #Pizzagate. Conspiracy theorists believed that Hillary Clinton, as part of a larger, criminal, pedophilic sex ring, was running part of the child sex trafficking ring out of the basement of a Washington, DC, pizza parlor. The allegations led to disastrous consequences when Edgar Maddison Welch

charged Comet Ping Pong with a rifle and handgun, and opened fire.[73] The campaign that led to the theory and the shooting, in contrast to its climactic outcome, has modest origins: two troll Reddit posts, a Sputnik reporter, and an Alt-Right activist.[74]

1. Background

The first critical precursor to the disinformation campaign was the hacking of Hillary Clinton's electoral campaign chair John Podesta (as well as others). Findings from the Mueller Report indicate that in March of 2016 the General Staff of the Russian Army (GRU) began a spearphishing (targeted phishing attacks) campaign on the Democratic Congressional Campaign Committee (DCCC), Democratic National Committee (DNC), and Hillary Clinton's electoral campaign staff gaining access to "tens of thousands of emails" from their victims.[75] By June of 2016, the DNC knew and publicly addressed the Russian intrusion into their networks roughly at the same time as the emails began to surface; the emails were circulated by two individuals under the pseudonyms DCLeaks and Guccifer 2.0, as well as through WikiLeaks.[76] While not particularly damning, the information contained personally identifiable information, financial information, campaign opposition research, and sensitive policy documents.[77] One email in particular, an invitation to a performance piece entitled Spirit Cooking by conceptual artist Marina Abramovic, however, was to set the stage for building the disinformation campaign.[78] The dinner invitation mentioned in the email "makes playful reference to one of Abramovic's past works" but was later taken completely out of context to insinuate darker ritualistic

[73] Petula Dvorak, "At a D.C. Pizzeria, the Dangers of Fake News Just Got All Too Real," *The Washington Post*, December 5, 2016, https://www.washingtonpost.com/local/at-a-dc-pizzeria-the-dangers-of-fake-news-just-got-all-too-real/2016/12/05/b8ae43b8-baf4-11e6-94ac-3d324840106c_story.html.

[74] Yochai Benkler, Robert Faris, and Hal Roberts, "The Propaganda Pipeline: Hacking the Core from the Periphery," in *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, ed. Yochai Benkler, Robert Faris, and Hal Roberts (Oxford University Press, 2018), 0, https://doi.org/10.1093/oso/9780190923624.003.0007.

[75] Mueller III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election Volume I and II," 37.

[76] Mueller III, 1, 42–49.

[77] Mueller III, 41, 43.

[78] Benkler, Faris, and Roberts, "The Propaganda Pipeline," 227.

behavior and served as a cornerstone for the #Pizzagate campaign.[79] In sum, these emails sparked a tidal wave of journalism, backlash, and research and were covered by everyone from the BBC to the *Los Angeles Times*.[80]

The second critical precursor was the back and forth between both major parties and their respectively uncritical journalists hurling sexual misconduct charges at their opponents throughout the 2016 electoral campaign, all of which surrounded Jeffrey Epstein, the prominent financier later found to be a sex offender. On the Republican side, Trump was accused of sexual assault of a minor at an event hosted by the late Epstein and, on the Democratic side, wild speculation surrounded both the Clintons and their association with Epstein.[81] These accusations amplified the disinformation campaign and, together with the leaked emails, provided the setting for the campaign.

2. Disinformation Campaign

The campaign itself was exceedingly simple, requiring only a light touch across several platforms and minor media insertion, and was sparked into motion by the Alt-Right movement. *The New York Times* produced a consolidated timeline of events starting with the initial hack of emails through the shooting (Figure 2); an examination of the disinformation campaign itself, however, principally occurs between the newspaper's steps four through six.[82]

---

[79] Eric Levitz, "Report: Clinton Linked to Satanic Rituals Involving Kidnapped Children and Marina Abramovic," *New York Magazine*, November 4, 2016, https://nymag.com/intelligencer/2016/11/spirit-cooking-explained-satanic-ritual-or-fun-dinner.html.

[80] BBC, "18 Revelations from Wikileaks' Hacked Clinton Emails," *BBC News*, October 14, 2016, sec. U.S. & Canada, https://www.bbc.com/news/world-us-canada-37639370; Chris Megerian and Michael A. Memoli, "What the WikiLeaks Emails Tell Us About Hillary Clinton's Campaign (And What They Don't)," *Los Angeles Times*, November 4, 2016, sec. Politics, https://www.latimes.com/politics/la-na-pol-wikileaks-explained-20161031-story.html.

[81] Yochai Benkler, Robert Faris, and Hal Roberts, "The Propaganda Feedback Loop," in *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, ed. Yochai Benkler, Robert Faris, and Hal Roberts (Oxford University Press, 2018), 91–97, https://doi.org/10.1093/oso/9780190923624.003.0003.

[82] Gregor Aisch, Jon Huang, and Cecilia Kang, "Dissecting the #PizzaGate Conspiracy Theories – The New York Times," *The New York Times*, December 10, 2016, https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html?mtrref=journals.plos.org&gwh=D807BE939430514 1EEE93AE68F9D65EC&gwt=pay&assetType=PAYWALL.

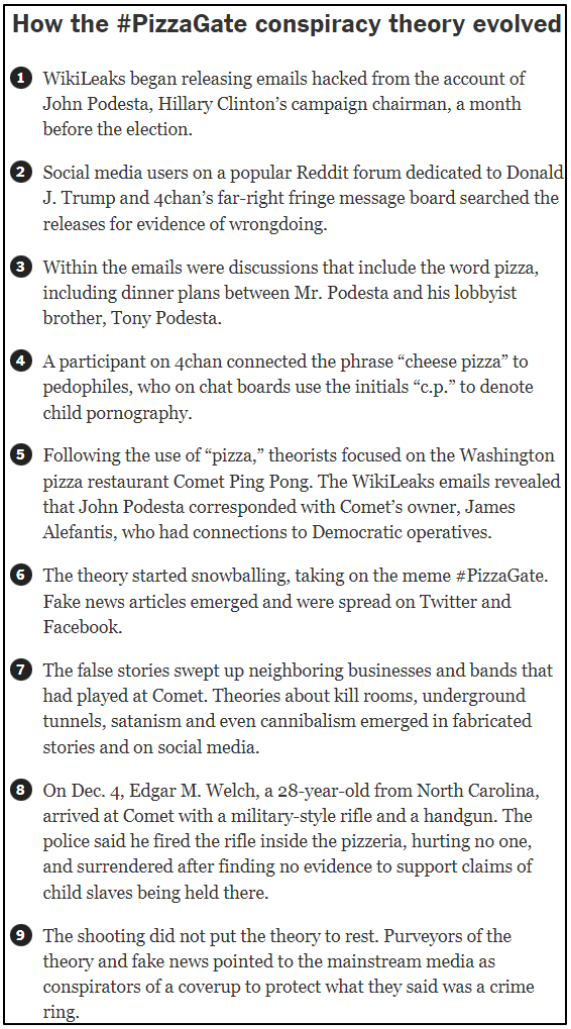


Figure 2. The *New York Times* chronology.[83]

The New York Times provides a starting point when examining the events but a more detailed look at the first connections between cheese pizza and child pornography (c.p. equated to c.p.), as well as "snowballing," reveal an intricate disinformation campaign. Benkler et al. fill in the details, tracing the campaign back to two Reddit posts on November 3rd, 2016: one instigating the connection between pizza mentioned in the leaked Podesta emails and pedophilia; the second a consolidation of like threads of information establishing a narrative.[84] From there, the information moved from Reddit to

[83] Source: Aisch, Huang, and Kang.

[84] Benkler, Faris, and Roberts, "The Propaganda Pipeline," 230.

Twitter. DiResta et al. detailed the use of nearly 4,000 Russian Internet Research Agency (IRA) "persona twitter accounts" and news bots to expand related hashtags among different demographics to increase the range of dissemination while varying the content to target separate audiences during the first days of the #Pizzagate campaign.[85] Metaxas and Finn, utilizing a tool called TwitterTrails, reverse engineered the timeline of #Pizzagate posts and found that the tweets including the hash tag originated at a no-longer-in-use troll Twitter account.[86] Subsequent retweets show that a second, minutes old, troll account was used to flood the "Turkish Twittersphere" prompting Turkish journalists to begin reporting on the #Pizzagate thread.[87] Through multiple sources the IRA, authentic users and inauthentic users flooded social media, expanding the dissemination of the narrative and bombarding media outlets to pick-up and report to a larger audience.

Parallel to the troll activity, two other people played a prominent role in furthering the narrative: Mike Cernovich, an Alt-Right activist, and Cassandra Fairbanks, a *Sputnik* reporter. Mike Cernovich, curator of the no longer available Alt-Right website Danger and Play, claimed Podesta's leaked Spirit Cooking dinner invitation was a darker occult ritual connected to a child trafficking conspiracy, Epstein, and the Clintons.[88] Now, a narrative began to emerge connecting the emails, pedophilia claims with Epstein, and the Clintons. Fairbanks, an American journalist who worked for Sputnik at the time but blogging under WeAreChange (a purported independent online media organization), posted two stories: the first, a graphic accounting of Marina Abramovic's performance pieces and second, a post connecting the disconnected threads from Reddit, Twitter, and Cernovich's piece.[89]

---

[85] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," *University of Nebraska – Lincoln*, U.S. Senate Documents, October 1, 2019, 84, https://digitalcommons.unl.edu/senatedocs/2.

[86] Panagiotis Metaxas and Samantha Finn, "The Infamous #Pizzagate Conspiracy Theory: Insight from a TwitterTrails Investigation," 2017, 3, https://repository.wellesley.edu/islandora/object/ir%3A300/datastream/PDF/view.

[87] Metaxas and Finn, 4.

[88] Mike Cernovich, "Podesta Emails Reveal Clinton's Inner Circle as Sex Cult with Connections to Human Trafficking," *Danger & Play* (blog), November 4, 2016, https://web.archive.org/web/20161104093838/http://www.dangerandplay.com/2016/11/03/podesta-emails-reveal-clintons-inner-circle-as-sex-cult-with-connections-to-human-trafficking/.

[89] Benkler, Faris, and Roberts, "The Propaganda Pipeline," 227–31.

It was Fairbanks' articles that were later used as sources traversing online and media outlets, moving from retweets by WikiLeaks to Infowars articles to the Drudge Report and ultimately to Sean Hannity's Fox program and news circulars the *Washington Times*.[90] Benkler et al. also note that between Fairbanks' release and the Infowars article between six and eight percent of the 76,127 related tweets were by accounts linked to three or more similar campaigns, although this was more "consistent with a background presence and continuous engagement of active Twitter accounts…than with a coordinated campaign to influence."[91]

From beginning to end, the #Pizzagate campaign is a careful stoking of political in-fighting and the political climate through Russian meddling rather than a fully Russian constructed disinformation campaign targeting Hillary Clinton. The novelty of the campaign is in the interchange between the Alt-Right movement's disinformation and Russian associated disinformation collectively building a more influential campaign in aggregation. Between the beginning of the campaign on November 3rd and the shooting on December 4th, little over a month had passed but the campaign had progressed rapidly with disastrous consequences.

3. The Campaign in Frame

#Pizzagate exploded into relevance in the course of a few days and rapidly developed a strong frame—expanding voluminously in the infosphere, borrowing credibility, and resonating deeply with the target audience—before the shooting caused a thorough look into the allegations framed by the campaign. The campaign skyrocketed from the Reddit user BedRiddenSam to source hacking national news coverage by Sean Hannity within 24-hours.[92]

[90] Benkler, Faris, and Roberts, 227–31.

[91] Benkler, Faris, and Roberts, 231–32.

[92] Benkler, Faris, and Roberts, 231. Source hacking is the process of manipulating a credible source, in this case Hannity and the Drudge report, into reporting disinformation as information, leveraging their credibility.

The campaign expanded rapidly due to the trolls, bots, publicity, and an audience in the far right searching for any misdeeds by the Clinton family. While there is no way to determine the individual effect of each category, the campaign's development was explosive. Metaxas and Finn ascribed the explosive growth and lack of scrutiny to online propagation in "a dense echo chamber, creating a perfect environment for growing the conspiracy theory."[93]

The campaign built on the tenuous connections of the Clintons and Epstein, and coded messages buried in "hidden documents," to create the illusion of credibility. Reporting by Fairbanks, Cernovich, WikiLeaks, InfoWars, the Drudge Report, and Sean Hannity expanded the viewership of the campaign to an even broader audience. The chain of reporting and reputation of each added to the credibility of the campaign.

The campaign had an accepting and, in this case, participatory audience. The Alt-Right movement actively helped build the conspiracy. Cernovich was quoted in *The New Yorker* stating '"If there's a story that can hurt Hillary, I want it in the news cycle" and knowingly contributed to the story's elevation to mainstream media channels.[94]

While it is unclear whether Cernovich and Fairbanks were complicit in the structured campaign or were themselves "Source Hacked" is unknown; however, the IRA linked accounts and source material provided by the GRU created a compelling narrative resulting in a violently successful campaign.

4. Counter Disinformation Campaign

Describing the counter disinformation for #Pizzagate is as simple as it is troubling: there was no counter disinformation campaign. Most of the available information comes from postmortem studies, larger in scope, covering 2016 election interference: the Mueller Report in 2019 and the Senate Select Committee on Intelligence *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election* in 2020. The only official mention

[93] Metaxas and Finn, "The Infamous #Pizzagate Conspiracy Theory: Insight from a TwitterTrails Investigation," 4.

[94] Andrew Marantz, "Trolls for Trump," *The New Yorker*, October 24, 2016, https://www.newyorker.com/magazine/2016/10/31/trolls-for-trump.

of the possibility of an influence campaign linking the Podesta email hack and the beginning of the disinformation campaign was the *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* which states:

> The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the U.S. election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there.[95]

The 2019 Mueller Report provides initial findings in electoral interference throughout the 2016 election campaign including the hack of the DNC, DCCC, and Clinton's campaign staff, the Netyksho indictment, and other investigations into interference operations.[96] The heavily redacted report only offers half a page of the 448 page document to the IRA's targeting of Hillary Clinton, indicating their attempts to marginalize her as an electoral candidate but offers no specific disinformation details. The Netyksho indictment was a result of the Mueller investigation citing criminal charges against 13 GRU officers responsible for the original hack enabling the campaign under the pseudonyms DCLeaks, Guccifer 2.0, and others, but does not indicate their complicity in further portions of the disinformation campaign—the case remains open.[97]

The first publicly available cybersecurity efforts relating to the scope of the intrusion were conducted in late 2016. Initial reaction to the hack that enabled the campaign and reporting to the public about the hack was stalled due to the political climate, perceived erosion of confidence in electoral process of the general public, attribution and

[95] DHS Press Office, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security," Government, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[96] Mueller III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election Volume I and II."

[97] Robert S. Mueller III, Netyksho Indictment, No. 1:18-cr-00215-ABJ (United States District Court for the District of Columbia June 13, 2018).

investigation of the source of the hack, and time and resources necessary to develop a policy response.[98] The outcome was the December 2016 *Joint Analysis Report* (JAR) produced by DHS and the FBI, with a follow up by DHS's National Cybersecurity and Communications Integration Center two months later. Both detailed Russian tactics and tropes in GRIZZLY STEPPE, their codename for the collective Russian activity, and an initial assessment by the collective Intelligence Community (IC) on the scope of Russian interference in the 2016 election. These actions occurred nearly two months after the #Pizzagate campaign had successfully taken off and one month after the resulting shooting.

A more detailed accounting of the perverse scope of disinformation efforts in the 2016 election was detailed by the Senate Select Committee on Intelligence in 2020 of which the #Pizzagate campaign was only a small part of a complex web of sophisticated campaigns. The report states: the "IRA's…general intent to foment and promote divisiveness and discord amongst the American populace is strongly evidenced," detailing their use of everything from targeted social media posts and paid advertisements across numerous social media platforms to manipulating Google's search algorithms.[99] The majority of the investigative efforts that uncovered the comprehensive network of campaigns came from internal audits by social media companies beginning in late 2017 that was then shared with the Intelligence Committee. In total, the social media companies identified over 6,000 inauthentic accounts and 50,000 bots operating between 2015 and 2018 linked to the IRA, accounting for nearly nine million unique posts and resulting in 365 million engagements with authentic users.[100] #Pizzagate, as it turned out, was part of much larger phenomenon and was actually a minor event when compared with the greater

[98] Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election" (United States Senate, November 10, 2020), vol. III pgs.13-24, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.

[99] Select Committee on Intelligence, vol. Volume II pgs. 40–62. The report details activity across Facebook, Instagram, Twitter, Google, YouTube, Reddit, Tumblr, LinkedIn, and even less popular social media platforms such as Pinterest, Medium, "Vine, Gab, Meetup, VKontakte, and LiveJoumal." "Even browser extensions, music applications, and games, like Pokemon [sic] Go were incorporated into the IRA' s influence operation."

[100] Select Committee on Intelligence, vol. Volume II pgs. 40–62.

complex web, not warranting a mention among the immense scope of the unredacted material.

5. The Counter-Campaign Framed

The lack of counter disinformation efforts to the #Pizzagate disinformation campaign and later understanding of the sophisticated network of influence operations thoroughly undermine the currently employed counter disinformation model. The scope and complexity of disinformation actors' actions avoided detection years after the 2016 campaigns had ended. The Intelligence Committee found that emerging technologies, artificial intelligence, micro-targeting, automation, and adaptive tactics dramatically increased the capability and anonymity of disinformation actors.[101]

The committee's investigation identified shortfalls throughout the information environment and nearly complete lack of government agency counter measure efforts. First, in addition to internal audits by social media companies, independent researchers like DiResta et al., cybersecurity firm FireEye, and investigative reporting by *The Wall Street Journal* identified more inauthentic accounts than the social media companies themselves found.[102] This highlights the continued adaptability of actors to avoid identification and denial countermeasures. Second, within the government, early counter disinformation efforts in fall of 2016 were outsourced by the FBI to employed contractors; the committee lamented that "the apparently outsourced nature of this work is troubling: it suggests FBI either lacked resources or viewed work in this vein as not warranting more institutionalized consideration."[103] The sweeping nature and abundance of these disinformation campaigns belies the currently employed deny, refute, riposte counter disinformation model even with increased coordination between the U.S. government, social media companies, and even

[101] Select Committee on Intelligence, 74–75. Micro-targeting is increasingly specific advertisement targeting by particular consumer demographics.

[102] Select Committee on Intelligence, 39, 49, 68.

[103] Permanent Select Committee on Intelligence, "Misinformation, Conspiracy Theories, and 'Infodemics': Stopping the Spread Online" (Washington, D.C.: U.S. House of Representatives, October 15, 2020), vol. II Pg. 73, https://www.congress.gov/116/meeting/house/111087/documents/HHRG-116-IG00-Transcript-20201015.pdf.

media partners demonstrated here by the delay between disinformation campaign elements and counter disinformation actions.

Problematically, the proliferation of disinformation infects authentic actors as well causing them to contribute to the spread of disinformation. The committee cited numerous engagements by the IRA to cause gatherings and protests, contribute money to Russian backed disinformation advertising campaigns, and source hacking of high-profile individuals like Roger Stone, Michael McFaul, and Sean Hannity that supported disinformation campaigns.[104] This manipulation of these actors turns not only journalists or officials but friends, neighbors, and colleagues into unwitting agents of disinformation campaigns, further impeding both deny and riposte aspects of the countermeasures model.

The current counter disinformation model, even if employed properly, could not manage the increasing sophistication and complexity of disinformation campaigns. Denial of information sphere access is undercut by ease of access and anonymity. Ability to refute the disinformation is complicated by the cacophony of overlapping campaigns, sheer volume of disinformation, and source or crowd hacking. Riposte is similarly challenged by anonymity and social hacking. While resources, integration, and response latency could increase countermeasure efficacy, the emergence of new technologies and adaptive responses cut both ways—benefiting disinformation actors as well as those who counter them.

This case clearly demonstrates failures in hypothesis one, disseminating factual information that did not target the disinformation was ineffective. No work was done to counter the #Pizzagate campaign in real time. And, although delayed, the investigations into and reporting of both the false claims and the network intrusion (that served as a cornerstone of the campaign) exposed the disinformation. However, it was too late as the campaign succeeded in spreading virally, sowing political discord, and resulted in a related shooting.

[104] Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," 40, 46–47, 57.

Hypothesis two, incorporating concepts from Framing theory—in particular the concepts of building a strong frame (volume, credibility, and resonance), is partially supported in examining this case. Principally, any response would increase all three elements of a strong frame but there are specific aspects of the disinformation campaign that demonstrate the vulnerability of resonance specifically. Postmortem analysis indicates the increasingly personalized nature of disinformation campaigns and the outcome demonstrates the centrality of resonance in building either a disinformation or counter disinformation narrative. A targeted narrative more directly integrates with targets' worldview, increasing acceptance of dis/information into their schema, and in some cases—like this one—significantly altering their behavior. The greater collection of parallel disinformation and influence efforts complicates the plausibility of creating increasingly specific counter measures that resonate with target demographics—in a similar way to the network of disinformation campaigns—and this is a significant area for potential exploration.

C. CONCLUSION

The #Pizzagate disinformation campaign and the response from both U.S. government agencies, and private sector demonstrate the increasing danger and susceptibility of the U.S. to influence operations. With the right environment, less than 24-hours is required from campaign inception to source hacking national news and less that one month before violent altercation. The campaign also demonstrated a rapid transition across social media platforms, complicating tracking of narrative progression. Russian actors used the charged political environment and popular media in an opportunistic matter to create a novel and compelling narrative that resonated with an engaged audience that further contributed to the dis-now-misinformation.[105]

With the benefit of hindsight, the immense scope of a complex network of campaigns takes shape. This campaign occurred in parallel to numerous others targeting all conceivable demographics. The web of campaigns, active simultaneously, exceeds the

[105] Disinformation being intentional distribution of false information to cause harm. Misinformation being the distribution of false information unintentionally.

inherent capacity of the whole of the U.S. government even with public and private partners acting together. The alarming capacity of disinformation actors can no longer be countered with the current model due to capacity issues, time constraints, and competing information mediums.

Micro-targeting by disinformation agents demonstrates the significance of creating a strong frame. Actors flooded multiple platforms with varieties of disinformation allowing it to propagate organically among target audiences. Anonymity protected the actors and leveraged organic proliferation to generate credibility among social circles and even traditional source hacking of news media. Targeted disinformation campaigns are *tailored* to groups' worldviews, aiding integration of disinformation into their schema. Disinformation campaigns, as demonstrated by #Pizzagate, are custom fit to cause disruption.

Hypothesis one is not supported. Ambient information does little to prevent the spread of disinformation. Disinformation pollutes the information sphere and affects pockets of the population despite the availability of accurate information that counters disinformation narratives. The sheer volume of today's information sphere prevents an information campaign from dissuading susceptible audiences from buying into disinformation.

The second hypothesis is supported in this case. The necessity for a strong frame in countermeasures is demonstrated by what made #Pizzagate, and disinformation campaigns in general, successful: expansive dissemination, enhanced credibility, and resonating with target audiences. Larger viewership of tailored countermeasures from dedicated professionals would likely aid in resistance to disinformation campaigns.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PLANDEMIC

A. INTRODUCTION

This chapter will examine a recent non-state medical disinformation campaign, and the tactics employed to counter it by U.S. agencies, and the frame that created both narratives. First, the campaign and the campaign's desired worldview (schema) will be analyzed. Following the contextual analysis, the types of deception and strong frame concepts (volume, credibility, and resonance) previously examined in Chapter I will be used to examine the disinformation campaign. Second, the countermeasures employed will be outlined and analyzed using the strong frame concepts. Lastly, hypothesis one, correcting only the false information, and hypothesis two, implementation of strong frame concepts can better support counter disinformation efforts, will then be applied.

This case, called Plandemic, was selected because it illustrates the ability of non-state actors to generate an extraordinarily complex campaign in today's information environment. Plandemic demonstrates complexity and adaptability to employed countermeasures and illustrates gaps in current measures used to combat disinformation.

B. DISINFORMATION CAMPAIGN

Technological changes and the ambiguity of the online information sphere blur the lines between misinformation and disinformation, and inhibit demonstration of straightforward, cohesive disinformation narratives; however, one video series, *Plandemic* illustrates all the hallmarks of a successful disinformation campaign.[106]

Plandemic, a series, aired as a purported documentary by filmmaker Mikki Willis, began circulating online in May of 2020 with the first self-titled episode.[107] Following the first film, a sequel, *Plandemic: Indoctornation,* was released 18 August of the same year.

---

106 Unintentional versus intentionally distributed false information.

107 "'Plandemic: Indoctornation' Video Rehashes Debunked Claims and Conspiracy Theories about the COVID-19 Pandemic and Vaccines," *Health Feedback* (blog), August 20, 2020, https://healthfeedback.org/plandemic-indoctornation-rehashes-debunked-claims-and-conspiracy-theories-about-the-covid-19-pandemic-and-vaccines/.

The video series features an interview style narrative with former scientist Judy Mikovits in the first video and financial analysist David Martin in the second. In both cases, the interviewees sat across from Mr. Willis, telling their story. Each video attempts to make a compelling argument about conspiracies surrounding the pandemic involving near-coincidences, the government, medical professionals, and public figures. The list of accusations is numerous: the original 26-minute film propagates medical disinformation and invokes deep state ideologies.[108] Mikovits misattributes reputable sources such as Dr. Greg Wolff's study, *Influenza vaccination and respiratory virus interference among Department of Defense personnel during the 2017–2018 influenza season,* claiming the study shows flu vaccinations increase odds of contracting COVID-19 when the study demonstrates the opposite.[109] The film went viral after its initial release on the 4th of May 2020 resulting in nearly 2.5 million views in the first two weeks alone.[110] Over the course of the remaining year, the hashtags #scamdemic and #plandemic were tweeted 227,067

[108] *Plandemic 1*, Plandemic, 2020, https://plandemicseries.com/. Specifically he claims: Animal and fetal testing propagates pathogens responsible for chronic diseases; The generated vaccinations are the wrong therapy (targeted treatment); 'Big pharma' targets and silences truth-tellers (decenters) such as Judy Mikovits through police state cronyism supported by HHS, DOJ, and the FBI; Doctors and hospitals received monetary motivation to attribute deaths to COVID-19; Global conspiracy allegations against medical professionals such as Dr. Anthony Fauci, Former Chief Medical Advisor to the President of United States; Dr. Robert Gallo; Dr. Ian Lipkin, Director of the Center for Infection and Immunity; and Dr. Robert Redfield, then Director for the Center for disease control and prevention (CDC); and government agencies such as U.S. Department of Health and Human Services (HHS); U.S. National Institute of Allergy and Infectious Diseases (NAIAD); the U.S. National Institutes of Health (NIH) Fort Detrick U.S. Army Research Institute on Infectious Disease; and the CDC's North Carolina and China's Wuhan laboratories surrounding the origin of AIDS research, weaponization of Ebola, and development of COVID-19; The removal of Hydroxychloroquine as a valid treatment option despite its success in treating similar contagions; Mask wearing reintroduces virions to the wearer causing reinfection; social media conspiracy to silence dissenters by removing content from their platforms.

[109] Greg G. Wolff, "Influenza Vaccination and Respiratory Virus Interference Among Department of Defense Personnel During the 2017–2018 Influenza Season," *Vaccine* 38, no. 2 (January 10, 2020): 350–54, https://doi.org/10.1016/j.vaccine.2019.10.005.

[110] Sheera Frenkel, Ben Decker, and Davey Alba, "How the 'Plandemic' Movie and Its Falsehoods Spread Widely Online," *The New York Times*, May 20, 2020, sec. Technology, https://www.nytimes.com/2020/05/20/technology/plandemic-movie-youtube-facebook-coronavirus.html.

times by 40,000 people and even shared by a prominent Republican in Ohio to her 20,000 followers.[111]

In his 75-minute follow-up video, *Plandemic: Indoctornation*, Willis doubles down on claims made it in his first video and expands his conspiracy arguments to attack criticisms and critics of his first film, claiming an even more elaborate framework.[112] Willis' follow-up film boasts a two million viewer live stream and has further propelled the Plandemic brand, leading to a website available in 15 languages, merchandising, a book, and soon, a third film.[113] This monetization coupled with the pending third installment indicate a willing audience which, although indirectly, indicates some relative success and extension of Willis' campaign.

C. THE CAMPAIGN IN FRAME

This disinformation campaign resembles an explosive mandala of false information. The campaign uses all six of Whaley's six categorical definitions of deception: masking, repackaging, dazzling, mimicking, inventing, and decoying.[114] In

[111] Heather D. Lanier et al., "Analyzing COVID-19 Disinformation on Twitter Using the Hashtags #scamdemic and #plandemic: Retrospective Study," *PLOS ONE* 17, no. 6 (June 22, 2022): e0268409, https://doi.org/10.1371/journal.pone.0268409; John Naughton, "How the 'Plandemic' Conspiracy Theory Took Hold," *The Observer*, May 23, 2020, sec. Opinion, https://www.theguardian.com/commentisfree/2020/may/23/how-the-plandemic-conspiracy-theory-took-hold.

[112] *PLANDEMIC: Indoctornation*, PLANDEMIC, 2020, https://plandemicseries.com/. Willis' growing list of conspiracy items includes: The circumspect timing of the Event 201 Global Pandemic Exercise scenario hosted by the Bill & Melinda Gates Foundation, Johns Hopkins University, and the World Economic Forum five months prior to the COVID-19 outbreak; Fact checking of his original video targeted the character of research Judy Mikovits but not the validity of her claims; Financial analysist David Martin outlines COVID related patents dating back as early as 1999; Cites a contradiction in U.S. code preventing patenting of naturally occurring pathogens vis-à-vis U.S. code allowing patents of man-made pathogens but insinuates breaches of biological warfare statutes; References apparent internal documents indicating the transfer of COVID-19 related materials from U.S. laboratories to Wuhan based laboratories; Attacks search engines claiming manipulation of search returns and undermines the credibility of search engine, social media, and fact checking bodies; References a fictious CIA operation titled Operation Mockingbird claiming that the CIA has infiltrated the news media and journalism industry to sway public opinion; Doubles down on the conspiracy generated in his previous film adding World Health Organization (WHO) Global Preparedness Monitoring Board and its Director Tedros Adhanom, China, the Bill and Malinda Gates and Clinton foundations, and the whole of western medicine; Claims governments the world over will use the health crisis to expand government authorities and create a police state; Vaccination research targets African American and, globally, African populations; Character assassination of Bill Gates; And propagandizes mainstream media as a tool for the cabal-esque agenda.

[113] Mikki Willis, "Plandemic," May 2020, https://plandemicseries.com/.

[114] Whaley, "Toward a General Theory of Deception," 182–85.

regard to masking and mimicking, Willis skillfully manipulates the appearance of documents and data to influence the audience to come to his contrived conclusions. Willis repackages events such as Event 201, a high-level pandemic preparedness exercise, and the relationships between medical experts and government bodies to dazzle the audience, amplifying existing conspiracy theories with "new evidence." He also frames efforts to combat his campaign as a global conspiracy to silence the truth.

This campaign is particularly problematic in two ways: first, source hacking evolved into crowd hacking; second, reliance on multiple established conspiracy theories increased its ability to resonate with a wider target audience.[115] Notably, not only did Willis' campaign source hack a prominent U.S. official, but also—leveraging the explosion of support from an unwitting population—created a crowd sourcing effect at the population level rather than intermediaries such as media or government officials. Secondly, by relying on established conspiracy theories like QAnon or Operation Mockingbird, Willis piggybacks on belief in those theories to purpose an evolution of existing conspiracies rather than an entirely new narrative. Nazar and Pieters found that this expanded the audience and confounded efforts to stymie the flow of disinformation, specifically by multiplying sources and links, this despite efforts to remove them which "amplified negative sentiments regarding vaccination and containment measures among conspiracy theorists."[116]

The Plandemic campaign demonstrates all three components of a strong frame: volume, credibility, and resonance. Crowd sourcing exponentially increased the range of the campaign and lent it credibility. The campaign leveraged purposed documents and expert testimonies to substantiate its claims. And lastly, reliance on existing conspiracy theories not only increased the credibility among fringe groups but exploited their beliefs

[115] Source hacking as previously outlined in Chapter I is the manipulation of a credible source into releasing disinformation as though it is information to leverage the credibility of the credible source. Crowd hacking is an evolution that utilizes the credibility of multiple actors, the crowd, rather than one acknowledged credible source.

[116] Shahin Nazar and Toine Pieters, "Plandemic Revisited: A Product of Planned Disinformation Amplifying the COVID-19 'Infodemic,'" *Frontiers in Public Health* 9 (2021): 649930, https://doi.org/10.3389/fpubh.2021.649930.

to present an evolution rather than an inception of new disinformation. Through artful manipulation and incorporation of existing fringe conspiracies, Willis creates a strong frame that resonated with larger and larger populations through multiple dissemination points.

D. COUNTER-DISINFORMATION CAMPAIGN

In a search of government websites related to health and human services—Department of Health and Human Services(HHS) and National Institute of Allergy and Infectious Diseases (NIAID)—and those that combat disinformation—DOS, DOJ, DHS, Cybersecurity and Infrastructure Security Agency (CISA)—no mention of this disinformation campaign appears. There is one mention, however, by the Adam Schiff, the then chair of the Permanent Select Committee on Intelligence. In his opening remarks during a meeting on online disinformation threats, he states only: "The notorious Plandemic video, which was rife with false, conspiratorial themes, and health misinformation about COVID-19, was boosted by QAnon supporters and earned some eight million views prior to removal from social media."[117] There are two possible explanations for the paucity of federal government efforts at counter-disinformation around this case: broader counter-disinformation approaches are being leveraged at the state level, or press and social media companies are bearing the majority of the counter-disinformation burden.

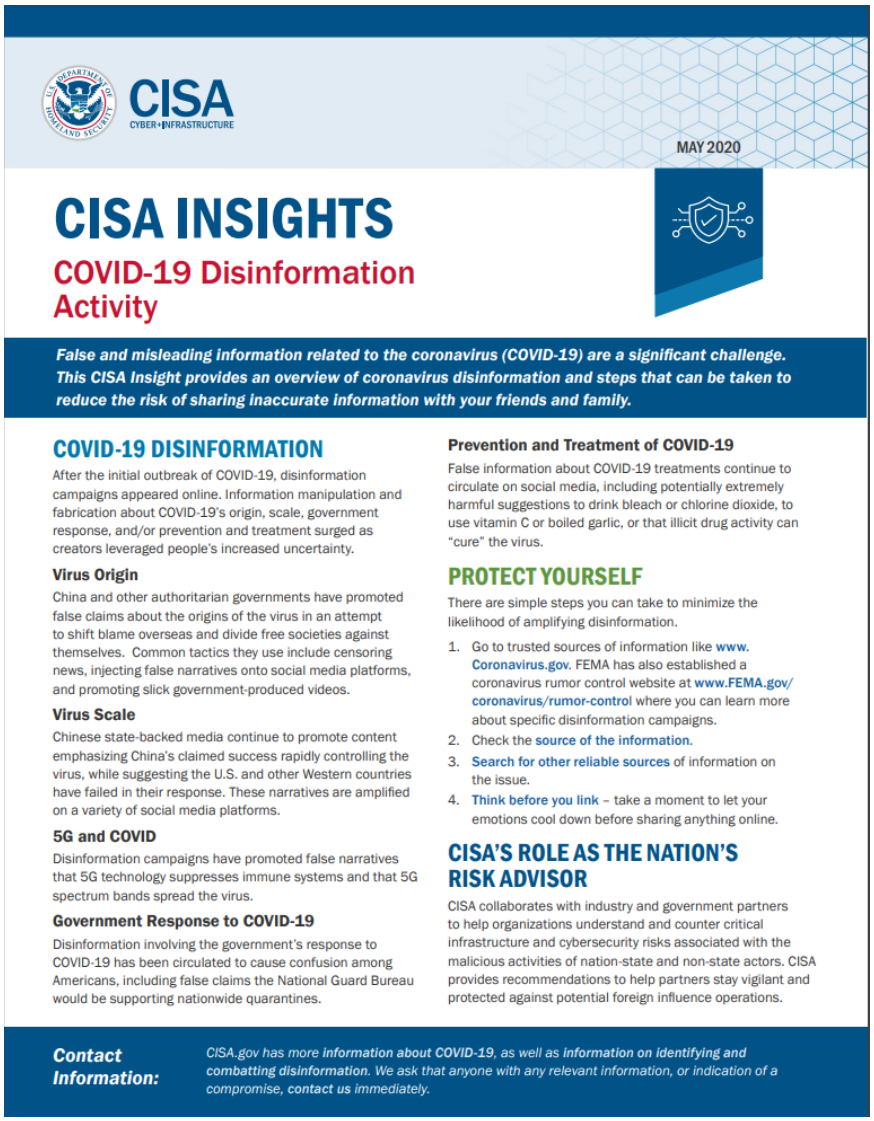
The most COVID-19 related counter-disinformation is available through CISA. CISA has released two products related to COVID-19 to boost public awareness of general COVID mis/disinformation: a COVID-19 disinformation toolkit (including a six-minute disinformation informative video and a three-page COVID-19 disinformation overview), and a one-page CISA INSIGHTS (Figure 3) reminiscent of the fact-based approached used by the Active Measures Working Group (AMWG) discussed in Chapter II (although

[117] Permanent Select Committee on Intelligence, "Misinformation, Conspiracy Theories, and 'Infodemics': Stopping the Spread Online," 4. QAnon related conspiracies were targeted, of which Plandemic was included, by YouTube, Facebook, and Twitter categorically. Facebook and Twitter began July of 2020 and YouTube October of the same year. No government intervention was indicated.

condensed).[118] These products are part of a greater list of releases to counter disinformation across numerous sectors like trafficking, COVID-19, foreign influence, mis/dis/malinformation, and bots. They also include novel, innovative engagement adaptations including comic strips to engage audiences, but these do not target specific disinformation campaigns.[119]

[118] Cybersecurity & infrastructure Security Agency, "COVID-19 Disinformation Toolkit," December 17, 2020, https://www.cisa.gov/covid-19-disinformation-toolkit; Cybersecurity & infrastructure Security Agency, "CISA Insights: COVID-19 Disinformation Activity," May 2020, https://www.cisa.gov/sites/default/files/publications/CISAInsights-COVID-19_Disinformation_Activity_508.pdf.

[119] Jamie Gorelick and Michael Chertoff, "Disinformation Best Practices and Safeguards Subcommittee Final Report Appendix 2," *Disinformation Best Practices and Safeguards Subcommittee*, August 24, 2022, 138, https://www.dhs.gov/sites/default/files/2022-08/22_0824_ope_hsac-disinformation-subcommittee-final-report-appendix-2_1.pdf.



CISA
CYBER • INFRASTRUCTURE

MAY 2020

CISA INSIGHTS

COVID-19 Disinformation Activity

False and misleading information related to the coronavirus (COVID-19) are a significant challenge. This CISA Insight provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.

COVID-19 DISINFORMATION

After the initial outbreak of COVID-19, disinformation campaigns appeared online. Information manipulation and fabrication about COVID-19's origin, scale, government response, and/or prevention and treatment surged as creators leveraged people's increased uncertainty.

Virus Origin

China and other authoritarian governments have promoted false claims about the origins of the virus in an attempt to shift blame overseas and divide free societies against themselves. Common tactics they use include censoring news, injecting false narratives onto social media platforms, and promoting slick government-produced videos.

Virus Scale

Chinese state-backed media continue to promote content emphasizing China's claimed success rapidly controlling the virus, while suggesting the U.S. and other Western countries have failed in their response. These narratives are amplified on a variety of social media platforms.

5G and COVID

Disinformation campaigns have promoted false narratives that 5G technology suppresses immune systems and that 5G spectrum bands spread the virus.

Government Response to COVID-19

Disinformation involving the government's response to COVID-19 has been circulated to cause confusion among Americans, including false claims the National Guard Bureau would be supporting nationwide quarantines.

Prevention and Treatment of COVID-19

False information about COVID-19 treatments continue to circulate on social media, including potentially extremely harmful suggestions to drink bleach or chlorine dioxide, to use vitamin C or boiled garlic, or that illicit drug activity can "cure" the virus.

PROTECT YOURSELF

There are simple steps you can take to minimize the likelihood of amplifying disinformation.

1. Go to trusted sources of information like **www.Coronavirus.gov**. FEMA has also established a coronavirus rumor control website at **www.FEMA.gov/coronavirus/rumor-control** where you can learn more about specific disinformation campaigns.
2. Check the **source of the information**.
3. **Search for other reliable sources** of information on the issue.
4. **Think before you link** – take a moment to let your emotions cool down before sharing anything online.

CISA'S ROLE AS THE NATION'S RISK ADVISOR

CISA collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. CISA provides recommendations to help partners stay vigilant and protected against potential foreign influence operations.

Contact Information: *CISA.gov has more **information about COVID-19**, as well as **information on identifying and combatting disinformation**. We ask that anyone with any relevant information, or indication of a compromise, **contact us** immediately.*

Figure 3. CISA INSIGHTS: COVID-19 Disinformation Activity[120]

The second explanation for the lack of federal government–led counter-disinformation effort is that the majority of the burden sharing for countering disinformation—in an information integrated environment—falls to platform creators and private and public partners to manage mis/disinformation internally (as insinuated by Schiff's opening remarks). Days after its release, journalists Yancey-Bragg and Shannon reported that the social media platforms Facebook, YouTube, and Twitter were "racing to

120 Source: Cybersecurity & infrastructure Security Agency, "CISA Insights: COVID-19 Disinformation Activity."

remove a slickly-produced interview with widely discredited scientist Judy Mikovits," but the video is still accessible on both platforms today.[121] An associated article by Rivera indicates that this was part of a larger effort by tech companies—Google, Microsoft, Facebook, Twitter, Reddit and their affiliated companies—to mitigate the general spread of COVID-19 mis/disinformation beginning in March of 2020.[122] Facebook's counter-disinformation efforts are now reported through their parent company, Meta. The *Coordinated Inauthentic Behavior Report*s in April of 2020 detail the removal of 24 Facebook pages, 35 Facebook accounts, and seven Facebook groups for "fake engagement, spam and artificial amplification" of COVID-19 related disinformation targeting the U.S. domestically in April; however, there were none in the December 2020 reports.[123] However, despite such efforts, Nina Jankowicz, disinformation fellow at the Wilson Center, admonished the Permanent Select Committee on Intelligence stating that "not only have the U.S. Government and social media platforms all but abdicated their responsibility to stop the threat of foreign disinformation, domestic disinformation now runs rampant."[124] The collective efforts of the U.S. government and social media platforms lacks the ability to concretely remove disinformation from online propagation through social media services.

The news media have taken an active role in exposing mis/disinformation surrounding Plandemic. Outlets including the *Guardian, The New York Times*, NPR, *USA Today,* and the *Washington Post*, as well as many others, have worked to expose the disinformation in the Plandemic series. This undermines the credibility of the purported

---

121 N'dea Yancey-Bragg and Joel Shannon, "Claim in Viral 'Plandemic' Video 'Could Lead to Imminent Harm,' Facebook Says," *USA TODAY*, May 9, 2020, https://www.usatoday.com/story/tech/2020/05/08/facebook-plandemic-judy-mikovits-shares-false-coronavirus-info/3095471001/.

122 Josh Rivera, "Coronavirus Brings Together Tech Companies against 'Misinformation,'" *USA Today* (blog), March 16, 2020, https://www.usatoday.com/story/tech/2020/03/16/coronavirus-tech-google-microsoft-facebook-misinformation/5064880002/.

123 Facebook, "April 2020 Coordinated Inauthentic Behavior Report" (Meta, April 2020), 2, 14, 16, https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf; Facebook, "December 2020 Coordinated Inauthentic Behavior Report" (Meta, December 2020), https://about.fb.com/wp-content/uploads/2021/01/December-2020-CIB-Report-.pdf.

124 Permanent Select Committee on Intelligence, "Misinformation, Conspiracy Theories, and 'Infodemics': Stopping the Spread Online," 12.

specialists, disarming the false arrest claims, providing research deflating the medical arguments, and exposing the association with QAnon related conspiracy theories.[125] Despite these efforts, Nazir and Pieters found that the Plandemic disinformation campaign can be considered a success due to wide dissemination through decentralized information sharing "subverting efforts to gatekeep its misinformation" and the magnification among conspiracy theorist communities.[126]

The collective counter-disinformation response in the wake of the Plandemic series has been lacking in all areas. There are indications of a concerted top-down approach integrating the U.S. government, social media companies, and traditional media outlets demonstrated by high level committee hearings, parent company reports, and the efforts detailed in Chapter 3 concerning integration following failures during the 2016 election, but the series has lost little traction.

E. THE COUNTER-CAMPAIGN FRAMED

In short, there has not been a coordinated counter-disinformation campaign to combat the Plandemic disinformation campaign. Rather, DHS, and the U.S. government Health and Human Services (HHS) enterprise has focused on providing accurate COVID-19 data and medical preventative methods (with the exception of the one-page flyer and linked "rumor control" webpage disseminated by CISA).[127] While the continued prevalence of COVID-19 in the U.S. does not indicate the ineffectiveness of U.S. government disinformation countermeasures, the lack of any agency's concerted efforts to

125 Naughton, "How the 'Plandemic' Conspiracy Theory Took Hold"; Davey Alba, "Virus Conspiracists Elevate a New Champion," *The New York Times*, May 9, 2020, sec. Technology, https://www.nytimes.com/2020/05/09/technology/plandemic-judy-mikovitz-coronavirus-disinformation.html?searchResultPosition=5; Scott Neuman, "Seen 'Plandemic'? We Take A Close Look At The Viral Conspiracy Video's Claims," *NPR*, May 8, 2020, sec. Coronavirus Live Updates, https://www.npr.org/2020/05/08/852451652/seen-plandemic-we-take-a-close-look-at-the-viral-conspiracy-video-s-claims; Yancey-Bragg and Shannon, "Claim in Viral 'Plandemic' Video 'Could Lead to Imminent Harm,' Facebook Says"; Katie Shepherd, "Who Is Judy Mikovits in 'Plandemic,' the Coronavirus Conspiracy Video Just Banned from Social Media?," *Washington Post*, May 8, 2020, https://www.washingtonpost.com/nation/2020/05/08/plandemic-judy-mikovits-coronavirus/.

126 Nazar and Pieters, "Plandemic Revisited."

127 Cybersecurity & infrastructure Security Agency, "CISA Insights: COVID-19 Disinformation Activity," 6.

counter the Plandemic campaign suggests two explanations: first, either a saturation of the disinformation environment and the inability for the U.S. to employ these methods individually; second, a shift in the counter-disinformation paradigm. The latter requires closer integration with social media industry in which the burden shifts from government measures to platform regulation measures.

The first argument belies the efficacy of the currently employed deny, refute, riposte model. The second argument shifts the cost and burden sharing to social media platforms and private enterprise but is still problematic. Social media platforms take an active role in the removal of disinformation content (deny) but due to crowd sourcing, the content remains available and continues to propagate. While the media and health sector attempt to correct the disinformation (refute) and undermine the credibility of Willis' and his "experts" (riposte), their efforts cannot penetrate groups with which the disinformation deeply resonates. This case illustrates the shortcomings of the deny, refute, riposte model even with expanded resources and latency improvement provided by burden sharing with private partners.

Aside from the media, the comprehensive effort of the HHS enterprise, public and private, to fight COVID-19 mis/dis/mal-information generally illustrates a clear depiction of hypothesis one (targeting only false information but not disinformation campaigns specifically). In other words, the majority of information produced to combat COVID-19 focused on fact-based information and focused little on disinformation campaigns as a whole. CISA's one-page flyer dismisses numerous forms of COVID-19 disinformation without specifically targeting any one source of disinformation. The consistent efforts of U.S. government officials and the health sector demonstrate moderate success with combatting COVID-19 as a public health emergency, but have little penetrative capacity on Willis' target audience. While attempting to broadly target dis/misinformation surrounding a health crisis is important and generally effective, the effectiveness of Willis' Plandemic campaign demonstrates two things: first, that not targeting the narratives of disinformation campaigns allows a campaign to flourish among target populations; second, this undermines social welfare measures put in place by the U.S. government and medical

professionals. This case demonstrates that hypothesis one has some effectiveness on the larger community but is ineffective against targeted groups.

In regard to hypothesis two, the comprehensive COVID-19 counter dis/ misinformation effort can be considered moderately successful in developing concepts of a strong frame—volume, credibility, and resonance—although these efforts were not directed specifically at the Plandemic campaign. For volume, the collective action of all partners in combating COVID-19 flooded the information sphere with factual data about the nature of COVID-19 and countermeasures to the virus. Separately, relating specifically to the Plandemic campaign, discrediting Willis, his experts, and correction of the disinformation presented was conducted by the press. Despite Willis' attempts, the credibility of numerous public health experts from around the world provides information that counter his claims. Willis attempts in his second installment to utilize tenuous connections among the medical expert community to undermine their collective credibility; however, their consistency in advising the public to inhibit the spread of COVID-19 remains. Resonance, that is alignment with the target audiences' worldview, is the primary outlier for the effectiveness of the Plandemic campaign; but the community with which Willis' campaign resonates represents only a fraction of the population. As Nazar and Pieter and Lanier et al. indicated, among the Plandemic target audience, the facts reported by media and medical experts that contradicted Willis' campaign did little to prevent the spread of disinformation.[128]

Counter disinformation efforts surrounding COVID-19 can be considered mostly successful in developing a strong frame when examining the impact on the population at large due in large part to the collective efforts of U.S. government officials, social media platforms, and media entities. However, the inability to resonate with the Plandemic disinformation campaign's target audience reduces the efficacy of measures countering the spread of COVID-19. This is due to negligence instilled in the target population by the disinformation campaign demonstrating both the significance of resonance in

[128] Nazar and Pieters, "Plandemic Revisited"; Lanier et al., "Analyzing COVID-19 Disinformation on Twitter Using the Hashtags #scamdemic and #plandemic."

disinformation campaigns and the necessity to employ resonance to increase counter-disinformation efforts. These findings are in line with hypothesis two.

F. CONCLUSION

The Plandemic disinformation campaign demonstrates the ability of even non-state actors to have a significant impact. The advent of social media has reduced the relative cost of creating and spreading disinformation in a way that challenges the U.S. government and partners in industry. Changes in the information environment—globally integrated internet access, smart phones, access to technologies, and social media platforms—have exponentially increased the speed and scope of both information and disinformation. These changes have reduced the efficacy of disinformation countermeasures due to the fact that they are reactive rather than proactive, and the size of the information environment limits the thorough denial of disinformation actor's access, speed, and disinformation proliferation.

The Plandemic campaign itself generated a compelling narrative with cohesive elements of a strong frame. The disinformation was spread by an uninformed audience. This highlights considerable complications with the transition from source hacking to crowd hacking. This social hacking increased the scope of dissemination and leveraged credibility of the audience with their friends, family, and social circles further strengthening the frame.[129] Willis' second installment demonstrated, again, the significant adaptability of successful disinformation campaigns.

In contrast, the development of a COVID-19 counter-disinformation effort presented a mixed success. U.S. government entities and medical experts provided voluminous credible COVID-19 information, but this information could not penetrate the disinformation campaign's influenced groups. The information simply did not resonate with influenced individuals.

Application of the hypotheses highlight some target areas where counter-disinformation efforts can be improved. The deny, refute, riposte model has become

[129] Social hacking is manipulation of social behaviors (e.g., crowd hacking).

distributed across multiple actors: the private sector became significantly more involved in the inhibiting (denial) the spread of disinformation, the U.S. government and health sector refuted disinformation claims, and the press undermined (riposte) the bad actors who were spreading disinformation. This distributed effort increases effectiveness of disinformation efforts. However, these efforts are weakened by the blurring of dis/misinformation through crowd hacking. Hypothesis one is supported in that accurate, fact-based information flooded the information sphere, combatting the spread of COVID-19 disinformation among the general population, but this method falls short in combatting the Plandemic disinformation campaign. Hypothesis two demonstrates a critical lack of resonance with the target audience; in a pandemic landscape, a lack of adherence to health protocols by any group undermines public health and reenforces the need to inhibit disinformation through resonance with target populations.

In comparing the relative success of the Plandemic disinformation campaign and the limited effectiveness of countermeasures, the most significant difference is targeted resonance with target audiences. Other avenues, like increasing resources for disinformation countermeasures, are impractical considering the relatively low cost required to generate modern campaigns because the cost of countermeasures will far exceed the cost of new disinformation campaigns, the volume of campaigns will exceed government capacity, and increasing of resources will not directly result in penetrative capacity to target audiences. There are two tactics that can be expanded, however, without requiring significantly more resources: *volume* and *resonance*. First, regarding volume, cooperative engagement with social media platforms can better support current disinformation efforts. And second, resonance requires targeting specific audiences with counter-disinformation tailored to their worldview (in a similar way to disinformation campaigns).

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS AND CONCLUSION

The information environment continues to be a battleground for competing narratives between positive actors such as the U.S. government who spread information, and negative actors such as Russia's Internet Research Agency, who spread disinformation. As the information sphere expands, the pathways and areas in which this information competition occurs continues to expand. U.S. agencies have continued to use the deny, refute, riposte counter disinformation model while disinformation actors have innovated disinformation efforts to circumvent counter disinformation efforts.[130] Integrating an understanding of framing, specifically incorporating strong frame development, can aid U.S. counter disinformation efforts by enhancing their effectiveness while maintaining the model's core concepts.

This concluding chapter synthesizes the information presented across the three cases and presents the insights along the axes of components of a strong frame (volume, credibility, and resonance). Recommendations to improve current U.S. government disinformation countermeasures follow the analysis. Finally, avenues of future research are discussed.

A. CASE OVERVIEW

The body of this thesis reviews the findings from three disinformation campaigns—Operation Denver, #Pizzagate (one campaign of note among the 2016 election Russian influence operations), and Plandemic campaigns—and the countermeasures employed by U.S. agencies and partners. Operation Denver was the 1980s Soviet disinformation campaign in which the U.S. was said to have manufactured HIV. Operation Denver's analysis provided a historical context for disinformation campaigns and early counter

[130] The deny, refute, riposte counter disinformation model is the three-pronged model used by U.S. agencies to counter disinformation. The first prong, deny, entails limiting access of disinformation actors to the disinformation space (e.g., removing of inauthentic social media accounts that spread disinformation). The second prong, refute, involves providing factual information to counter disinformation claims (e.g., providing a COVID-19 disinformation guide to counter disinformation about COVID-19 as seen in Chapter IV). The third prong, riposte, is the attribution and discreditation of a disinformation actor (e.g., identifying the source of HIV disinformation stemming from Soviet influence as seen in Chapter II).

disinformation efforts. The #Pizzagate campaign was an elaborate concoction linking the Clintons to the ongoing investigation into Jeffrey Epstein's sex trafficking case, occult rituals, and child pornography. The #Pizzagate campaign analysis illustrates how counter disinformation efforts have failed to adapt to the evolving information sphere due to the influence of the internet and social media. The final case, Plandemic, is a video series from director Mikki Willis undermining COVID-19 countermeasures and contriving COVID-19 measures as the work of a global medical and government cabal. The Plandemic analysis demonstrates the effectiveness of even non-state actors to conduct successful disinformation campaigns with significant social ramifications.

B. ANALYSIS

These three sample cases demonstrate the range of actions of both disinformation actors and counter disinformation efforts employed by the U.S. government. Notably, the latter two cases illustrate the inability for current counter disinformation efforts to keep pace with the efforts of a variety of disinformation actors in the ever-expanding information environment. Hypothesis one, which argues that focusing on dissemination of correct information effectively counters disinformation, was not supported in all cases. In the best case, factual dissemination of accurate information was effective at a whole-of-society level but was unable to influence affected target populations. Hypothesis two, which argues the efficacy of strong frame concepts, was supported to varying degrees in all cases. Each aspect of the strong frame concept merits further examination due to the way in which each contributed differently across the three examined cases.

a. Volume

Limiting access to the information environment is extremely difficult; rather, the information environment is an echo chamber in which the most "noise" leads to influence. The findings from Operation Denver's proliferation among countries with little to no ability to challenge claims, #Pizzagate's Twitter echo chamber, and Plandemic's grass roots mobilization are all indicative of Jack's research describing flooding of public

forums.[131] In all three cases, efforts were made to limit the access of disinformation actors to the information environment, but access could not be wholly denied. Further, recent changes in the information environment, namely internet access and growth of available platforms, complicate countermeasure efforts by increasing the avenues through which disinformation can reach intended audiences. These changes also expand the space of the competition among multiple, sometimes overlapping, mediums and platforms available to end users.

With the complications to denial in the deny, refute, riposte model, adjusting the volume of information to refute disinformation becomes the next greatest alternative. Clear indications of the importance of volume are represented in all three cases: the traction the Active Measures Working Group's (AMWG) report received only *after* the Gorbachev-Schultz exchange regarding Operation Denver, the post-shooting debunking in #Pizzagate, and the wide and thorough dissemination of general COVID-19 information throughout the pandemic. These findings illustrate the necessity to more carefully consider the principal target audience and tailor dissemination of information to maximize their viewership.

b. Credibility

The importance of credibility of information actors was demonstrated in the negative, meaning that in all three cases disinformation actors sought to reduce the credibility of countermeasure enablers to reduce their efficacy. Early in the AMWG's career, they learned this hard lesson.[132] In both the #Pizzagate and Plandemic campaigns, the disinformation actor actively sought to undermine the credibility of actors who would repudiate the allegations against them as a part of their campaign. In all three cases, the goal of the disinformation actor was to destroy the credibility of their targets and supplant their own narrative of events into the information sphere.

---

131 Jack, "Lexicon of Lies: Terms for Problematic Information," 9.

132 Schoen and Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 43. At a press conference a high-level TASS official dismantled the AMWG's analysis, undermining their credibility. (No date given)

A second demonstration of the influence of credibility is that the source hacking used in campaigns greatly boosted disinformation actor narrative credibility. From *Patriot* to Hannity and in using professional titles such as M.D. or financial analysist, disinformation actors borrowed credible titles to spread disinformation. In stark contrast to U.S. agents, disinformation actors needed no credibility while, once impinged, the U.S. agents operated with reduced efficacy.

A third demonstration of credibility's influence is the social engineering present in the latter two campaigns. Both cases used source hacking innovatively to hack crowd sentiment to propel disinformation through what appeared to be grassroots movements. These cases demonstrated that local credibility—influence among friends, colleagues, neighbors, and family—was an effective means to further increase the spread of disinformation.

c. Resonance

This last concept of a strong frame, resonance, demonstrated a high degree of significance in each case. The lasting effects among the African American community linked to Operation Denver, the closed echo chamber and shooting related to #Pizzagate, and the grassroots dissemination and association with QAnon conspiracy theorists in the Plandemic campaign demonstrate both the lasting and abrupt effects of resonance. Resonance, in these cases, not only contributed to an erosion of confidence in established U.S. institutions but also a call to action in at least one case.

The counter disinformation campaigns, in contrast, lacked these high degrees of resonance with the targeted audiences of disinformation campaigns. In Operation Denver, the primary targets of the disinformation campaign were the public, more specifically disenfranchised groups. The counter disinformation campaign, however, was broad spectrum and efforts by the AMWG were geared towards information intermediaries—the press, professionals, and foreign intelligence services—to control disinformation propagation. There was a mismatch in targeting between the disinformation campaign and the counter measures employed. In the latter two cases, the disinformation spread so

quickly that countermeasures were not effectively employed, and retroactive countermeasure efforts were unable to penetrate the highly reticent target populations.

C. RECOMMENDATIONS

As the information environment continues to change, disinformation actors actively expand their repertoire of disinformation activities and methods; U.S. agencies should likewise expand counter disinformation methods. Incorporating aspects of a strong frame from framing theory provides a relatively low-tech opportunity for improvement of the currently employed model. The recommendations that follow deviate little from the currently used deny, refute, riposte model; instead, they seek to improve the model by tailoring currently employed countermeasure efforts.

a. Social Media Integration – A Distributed Information Model

In addition to the existing partnership between industry and U.S. agencies, U.S. agencies can work with industry partners to take an active role in information sharing to increase the volume of factual information propagation.[133] Rather than denial of disinformation actor access or tracking and reporting to U.S. agencies, the active role would be to disseminate factual information in coordination with social media platform algorithms otherwise used for monetization, partisan news, and advertisements tailored to end users. These algorithms are designed to tailor ad placement and information to specific end users' preferences and can assist distribution with maximized resonance, with the cooperation of social media partners (and end user licensing agreements). Admittedly, replacing content that generates ad revenue with factual information provided by U.S. agencies would require significant negotiation with social media companies to account for fiscal losses.

[133] Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," vol. II p.78-79. These cooperative efforts are defensive in nature and include: reporting and identification of violent extremism, forum activities to protect digital rights, disruption of cyber-crime and removal of extremist propaganda, and tracking financial criminal behavior. On an ad hoc basis, cooperation also exists to boost transparency (to both the federal government and end users), and cooperation in "exposure of malign information operations."

b. Community Partnerships

A limitation presented by disinformation campaigns is the undermining of information actors; however, like counter disinformation measures, the discredited targets are often in prominent positions at the federal level. In both the #Pizzagate and Plandemic campaigns, we can see that the targets were either at the federal level or on a global level. Like the crowd hacking employed by the latter two campaigns, information sharing can be distributed to lower levels unaffected by discreditation, not at a local or state government level but rather community leaders of targeted or at-risk groups. These partnerships would be established by federal agencies and local contingents to build a distributed network of partnerships, fundamentally altering the information dissemination process. Building partnerships with community leaders increases both the credibility of the information actor and incorporates an intermediary to adjust information in a positive manner that better resonates with target audiences who would otherwise be susceptible to tailored disinformation campaigns. Rather than a stop-gap measure, building trust and cooperation at this level takes time and effort but diminishes the susceptibility of at-risk communities long-term.

D. FUTURE RESEARCH

Disinformation actors, whether state or non-state actors, will continue to target U.S. institutions, and U.S. agencies will continue to defend the American people from the discord and disruptive influence of these actors. Framing and narratives will continue to be the mode of competition throughout the voluminous information sphere. As such, researching effective components of both information and disinformation campaigns should be studied to bolster future counter disinformation efforts. Further research would incorporate social fault lines to determine likely targets of disinformation campaigns to preempt such efforts. A more technical avenue of future research is the effect of established and emerging technologies (e.g., social media algorithms and AI tools like ChatGPT) on framing of information but how these tools can contribute to U.S. agency countermeasures.

E. CONCLUSION

This thesis has contrasted disinformation and counter disinformation narratives and methods and argued that the U.S. government's counter disinformation model has become largely ineffective. Counter disinformation efforts can be improved by incorporating framing theory into disinformation countermeasure planning and execution. Rather than changing the counter disinformation model, this thesis proposes using framing theory to increase the efficacy of employed measures.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Aiken, Alex. "RESIST 2 Counter-Disinformation Toolkit." *Government Communication Service*, 2021, 60. https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf.

Aisch, Gregor, Jon Huang, and Cecilia Kang. "Dissecting the #PizzaGate Conspiracy Theories – The New York Times." *The New York Times*, December 10, 2016. https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html?mtrref=journals.plos.org&gwh=D807BE9394305141EEE93AE68F9D65EC&gwt=pay&assetType=PAYWALL.

Alba, Davey. "Virus Conspiracists Elevate a New Champion." *The New York Times*, May 9, 2020, sec. Technology. https://www.nytimes.com/2020/05/09/technology/plandemic-judy-mikovitz-coronavirus-disinformation.html?searchResultPosition=5.

Allenby, Brad, and Joel Garreau. "Weaponized Narrative Is the New Battlespace." Defense One, January 3, 2017. https://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/.

Arif, Ahmer, Kelley Shanahan, Fang-Ju Chou, Yoanna Dosouto, Kate Starbird, and Emma S. Spiro. "How Information Snowballs: Exploring the Role of Exposure in Online Rumor Propagation." In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 466–77. CSCW '16. New York, NY, USA: Association for Computing Machinery, 2016. https://doi.org/10.1145/2818048.2819964.

Barker, David C. "Values, Frames, and Persuasion in Presidential Nomination Campaigns." *Political Behavior* 27, no. 4 (2005): 375–94. https://doi.org/10.1007/s11109-005-8145-4.

Bayer, Judit, Natalija Bitiukova, Petra Bard, Judit Szakács, Alberto Alemanno, and Erik Uszkiewicz. "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, February 1, 2019. https://doi.org/10.2139/ssrn.3409279.

BBC. "18 Revelations from Wikileaks' Hacked Clinton Emails." *BBC News*, October 14, 2016, sec. U.S. & Canada. https://www.bbc.com/news/world-us-canada-37639370.

Benkler, Yochai, Robert Faris, and Hal Roberts. "The Propaganda Feedback Loop." In *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, edited by Yochai Benkler, Robert Faris, and Hal Roberts, 0. Oxford University Press, 2018. https://doi.org/10.1093/oso/9780190923624.003.0003.

———. "The Propaganda Pipeline: Hacking the Core from the Periphery." In *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, edited by Yochai Benkler, Robert Faris, and Hal Roberts, 0. Oxford University Press, 2018. https://doi.org/10.1093/oso/9780190923624.003.0007.

Bernays, Edward L. *Propaganda*. New York: Ig Publishing, 2005.

Bogart, Laura M., and Sheryl Thorburn. "Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention Among African Americans?" *JAIDS Journal of Acquired Immune Deficiency Syndromes* 38, no. 2 (February 1, 2005): 213. https://journals.lww.com/jaids/fulltext/2005/02010/are_hiv_aids_conspiracy_beliefs_a_barrier_to_hiv.14.aspx.

Bradshaw, Samantha, and Philip N Howard. "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," 2019, 27. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1209&context=scholcom.

Canan, Mustafa, and Anthony Akil. "A Warfare Domain Approach to the Disinformation Problem," March 2020, 82–91. https://www.proquest.com/openview/0b9049cf147a8a355400012a72755a4a/1?pq-origsite=gscholar&cbl=396500.

Cernovich, Mike. "Podesta Emails Reveal Clinton's Inner Circle as Sex Cult with Connections to Human Trafficking." *Danger & Play* (blog), November 4, 2016. https://web.archive.org/web/20161104093838/http://www.dangerandplay.com/2016/11/03/podesta-emails-reveal-clintons-inner-circle-as-sex-cult-with-connections-to-human-trafficking/.

Chong, Dennis, and James N. Druckman. "A Theory of Framing and Opinion Formation in Competitive Elite Environments." *Journal of Communication* 57, no. 1 (2007): 99–118. https://doi.org/10.1111/j.1460-2466.2006.00331.x.

———. "Framing Theory." *Annual Review of Political Science* 10, no. 1 (June 1, 2007): 103–26. https://doi.org/10.1146/annurev.polisci.10.072805.103054.

Colley, Thomas Paul, Francesca Granelli, and Jente Althuis. "Disinformation's Societal Impact: Britain, COVID and Beyond." *Defence Strategic Communications* 8, no. 1 (July 3, 2020): 89–140. https://doi.org/10.30966/2018.RIGA.8.3.

Cybersecurity & infrastructure Security Agency. "CISA Insights: COVID-19 Disinformation Activity," May 2020. https://www.cisa.gov/sites/default/files/publications/CISAInsights-COVID-19_Disinformation_Activity_508.pdf.

———. "COVID-19 Disinformation Toolkit," December 17, 2020. https://www.cisa.gov/covid-19-disinformation-toolkit.

Daniel, Donald C., and Katherine L. Herbig. "Propositions on Military Deception." *Journal of Strategic Studies* 5, no. 1 (March 1, 1982): 155–77. https://doi.org/10.1080/01402398208437105.

Department of Homeland Security. "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 2019, 28. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

Department of Homeland Security Press Office. "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security." Government, October 7, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics & Tropes of the Internet Research Agency." *University of Nebraska – Lincoln*, U.S. Senate Documents, October 1, 2019, 103. https://digitalcommons.unl.edu/senatedocs/2.

Donovan, Joan, and Brian Friedberg. "Source Hacking," 56. Accessed May 21, 2022. https://datasociety.net/wp-content/uploads/2019/09/Source-Hacking_Hi-res.pdf.

Druckman, James N. "The Implications of Framing Effects for Citizen Competence." *Political Behavior* 23, no. 3 (2001): 225–56. https://doi.org/10.1023/A:1015006907312.

Dvorak, Petula. "At a D.C. Pizzeria, the Dangers of Fake News Just Got All Too Real." *The Washington Post*, December 5, 2016. https://www.washingtonpost.com/local/at-a-dc-pizzeria-the-dangers-of-fake-news-just-got-all-too-real/2016/12/05/b8ae43b8-baf4-11e6-94ac-3d324840106c_story.html.

Erbschloe, Michael. *Extremist Propaganda in Social Media: A Threat to Homeland Security*. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2019.

Facebook. "April 2020 Coordinated Inauthentic Behavior Report." Meta, April 2020. https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf.

———. "December 2020 Coordinated Inauthentic Behavior Report." Meta, December 2020. https://about.fb.com/wp-content/uploads/2021/01/December-2020-CIB-Report-.pdf.

Frenkel, Sheera, Ben Decker, and Davey Alba. "How the 'Plandemic' Movie and Its Falsehoods Spread Widely Online." *The New York Times*, May 20, 2020, sec. Technology. https://www.nytimes.com/2020/05/20/technology/plandemic-movie-youtube-facebook-coronavirus.html.

Gillette, Robert. "AIDS: A Global Assessment : Soviets Suggest Experiment Leaks in U.S. Created the AIDS Epidemic." *Los Angeles Times*, August 9, 1987. https://www.latimes.com/archives/la-xpm-1987-08-09-ss-592-story.html.

Gorelick, Jamie, and Michael Chertoff. "Disinformation Best Practices and Safeguards Subcommittee Final Report Appendix 2." *Disinformation Best Practices and Safeguards Subcommittee*, August 24, 2022, 138. https://www.dhs.gov/sites/default/files/2022-08/22_0824_ope_hsac-disinformation-subcommittee-final-report-appendix-2_1.pdf.

Haider-Markel, Donald P., and Mark R. Joslyn. "Gun Policy, Opinion, Tragedy, and Blame Attribution: The Conditional Influence of Issue Frames." *The Journal of Politics* 63, no. 2 (2008): 520–43. https://doi.org/10.1111/0022-3816.00077.

Jack, Caroline. "Lexicon of Lies: Terms for Problematic Information." Data & Society Research Institute, 2017. https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf.

Korta, Samantha M. "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security," March 2018, 154. https://calhoun.nps.edu/bitstream/handle/10945/58322/18Mar_Korta_Samantha.pdf?sequence=1&isAllowed=y.

Lanier, Heather D., Marlon I. Diaz, Sameh N. Saleh, Christoph U. Lehmann, and Richard J. Medford. "Analyzing COVID-19 Disinformation on Twitter Using the Hashtags #scamdemic and #plandemic: Retrospective Study." *PLOS ONE* 17, no. 6 (June 22, 2022): e0268409. https://doi.org/10.1371/journal.pone.0268409.

Levitz, Eric. "Report: Clinton Linked to Satanic Rituals Involving Kidnapped Children and Marina Abramovic." *New York Magazine*, November 4, 2016. https://nymag.com/intelligencer/2016/11/spirit-cooking-explained-satanic-ritual-or-fun-dinner.html.

Marantz, Andrew. "Trolls for Trump." *The New Yorker*, October 24, 2016. https://www.newyorker.com/magazine/2016/10/31/trolls-for-trump.

Megerian, Chris, and Michael A. Memoli. "What the WikiLeaks Emails Tell Us About Hillary Clinton's Campaign (And What They Don't)." *Los Angeles Times*, November 4, 2016, sec. Politics. https://www.latimes.com/politics/la-na-pol-wikileaks-explained-20161031-story.html.

Metaxas, Panagiotis, and Samantha Finn. "The Infamous #Pizzagate Conspiracy Theory: Insight from a TwitterTrails Investigation," 2017. https://repository.wellesley.edu/islandora/object/ir%3A300/datastream/PDF/view.

Moy, Wesley R, and Kacper Gradon. "COVID-19 Effects and Russian Disinformation Campaigns," no. 2020 (2020): 28. https://www.hsaj.org/articles/16533.

Mueller III, Robert S. Netyksho Indictment, No. 1:18-cr-00215-ABJ (United States District Court for the District of Columbia June 13, 2018).

———. "Report on the Investigation into Russian Interference in the 2016 Presidential Election Volume I and II." U.S. Department of Justice, March 2019. https://www.justice.gov/archives/sco/file/1373816/download.

Naughton, John. "How the 'Plandemic' Conspiracy Theory Took Hold." *The Observer*, May 23, 2020, sec. Opinion. https://www.theguardian.com/commentisfree/2020/may/23/how-the-plandemic-conspiracy-theory-took-hold.

Nazar, Shahin, and Toine Pieters. "Plandemic Revisited: A Product of Planned Disinformation Amplifying the COVID-19 'Infodemic.'" *Frontiers in Public Health* 9 (2021): 649930. https://doi.org/10.3389/fpubh.2021.649930.

Neuman, Scott. "Seen 'Plandemic'? We Take A Close Look At The Viral Conspiracy Video's Claims." *NPR*, May 8, 2020, sec. Coronavirus Live Updates. https://www.npr.org/2020/05/08/852451652/seen-plandemic-we-take-a-close-look-at-the-viral-conspiracy-video-s-claims.

Perkins, Alexander M. "Soviet Active Measures Reborn for the 21st Century: What Is to Be Done?," December 2018. https://calhoun.nps.edu/handle/10945/61246.

Permanent Select Committee on Intelligence. "Misinformation, Conspiracy Theories, and 'Infodemics': Stopping the Spread Online." Washington, D.C.: U.S. House of Representatives, October 15, 2020. https://www.congress.gov/116/meeting/house/111087/documents/HHRG-116-IG00-Transcript-20201015.pdf.

Plandemic 1. Plandemic, 2020. https://plandemicseries.com/.

PLANDEMIC: Indoctornation. PLANDEMIC, 2020. https://plandemicseries.com/.

Health Feedback. "'Plandemic: Indoctornation' Video Rehashes Debunked Claims and Conspiracy Theories about the COVID-19 Pandemic and Vaccines," August 20, 2020. https://healthfeedback.org/plandemic-indoctornation-rehashes-debunked-claims-and-conspiracy-theories-about-the-covid-19-pandemic-and-vaccines/.

Polletta, Francesca, and M. Kai Ho. "Frames and Their Consequences." In *The Oxford Handbook of Contextual Political Analysis*, 2006. https://doi.org/10.1093/oxfordhb/9780199270439.003.0010.

Rivera, Josh. "Coronavirus Brings Together Tech Companies against 'Misinformation.'" *USA Today* (blog), March 16, 2020. https://www.usatoday.com/story/tech/2020/03/16/coronavirus-tech-google-microsoft-facebook-misinformation/5064880002/.

Schoen, Fletcher, and Christopher J Lamb. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference." *Institute for National Strategic Studies* No. 11 (June 2012): 155. https://ndupress.ndu.edu/portals/68/documents/stratperspective/inss/strategic-perspectives-11.pdf.

Select Committee on Intelligence. "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election." United States Senate, November 10, 2020. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.

Selvage, Douglas, trans. "KGB, Information Nr. 2955 [to Bulgarian State Security]." Wilson Center Digital Archive, Committee for Disclosing the Documents and Announcing the Affiliation of Bulgarian Citizens to the State Security and the Intelligence Services of the Bulgarian National Army (CDDAABCSSISBNA-R), September 7, 1985. F. 9, op. 4, a.e. 663. https://digitalarchive.wilsoncenter.org/document/102957/download.

Selvage, Douglas. "Operation 'Denver': The East German Ministry for State Security and the KGB's AIDS Disinformation Campaign, 1986–1989 (Part 2)." *Journal of Cold War Studies* 23, no. 3 (2021): 4–80. https://muse.jhu.edu/pub/6/article/801905.

Selvage, Douglas, and Christopher Nehring. "Operation 'Denver': KGB and Stasi Disinformation Regarding AIDS | Wilson Center." *Operation "Denver": KGB and Stasi Disinformation Regarding AIDS* (blog), July 22, 2019. https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids.

Shepherd, Katie. "Who Is Judy Mikovits in 'Plandemic,' the Coronavirus Conspiracy Video Just Banned from Social Media?" *Washington Post*, May 8, 2020. https://www.washingtonpost.com/nation/2020/05/08/plandemic-judy-mikovits-coronavirus/.

Simchayoff, Elad. "Operation Infektion." *Lessons from History* (blog), July 30, 2020. https://medium.com/lessons-from-history/operation-infektion-a1485fe85443.

Sniderman, Paul M., and Sean M. Theriault. "Chapter 5 The Structure of Political Argument and the Logic of Issue Framing." In *Studies in Public Opinion: Attitudes, Nonattitudes, Measurement Error, and Change*, 133–65. Princeton University Press, 2004. https://doi.org/10.2307/j.ctv346px8.

Starbird, Kate, Ahmer Arif, and Tom Wilson. "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations." *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 7, 2019): 1–26. https://doi.org/10.1145/3359229.

Sun Tzu. *The Art of War*. UNESCO Collection of Representative Works. Chinese Series. London: New York, 1971.

Tankard Jr., James W. "Chapter 4: The Empirical Approach to the Study of Media Framing." In *Framing Public Life: Perspectives on Media and Our Understanding of the Social World*, edited by Stephen D. Reese, Oscar H. Gandy Jr, and August E. Grant, 95–105. Routledge, 2001.

United States Department of State. "Foreign Affairs Note: The U.S.S.R.'s AIDS Disinformation Campaign." U.S. Department of State, July 1987. https://books.google.com/books?id=kWhpAAAAMAAJ&pg=PA4&source=gbs_selected_pages&cad=2#v=onepage&q&f=false.

———. "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87," August 1987. https://books.google.com/books?hl=en&lr=&id=JaZv3QJCdKMC&oi=fnd&pg=PR8&dq=%22Soviet+Influence+Activities:+A+Report+on+Active+Measures+and+Propaganda,+1986+-+87%22&ots=RF-Z_m6duF&sig=hAYCl9vu8bmhVHBWOjgaS02QcLc#v=onepage&q=%22Soviet%20Influence%20Activities%3A%20A%20Report%20on%20Active%20Measures%20and%20Propaganda%2C%201986%20-%2087%22&f=false.

U.S. State Department Global Engagement Center. "GEC Counter-Disinformation Dispatches # 1 – A Counter-Disinformation System That Works," January 8, 2020. https://e.america.gov/t/ViewEmail/i/9146D16121A6D6562540EF23F30FEDED/981423FE1274E8AFBA4AF9908B8D85ED.

———. "GEC Counter-Disinformation Dispatches # 2 – Three Ways to Counter Disinformation," February 11, 2020. https://e.america.gov/t/ViewEmail/i/95383D12423453CD2540EF23F30FEDED/5069D0DCBA89C0A1EBAD456BEB5F1DD6.

———. "Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem," January 2022, 33. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (March 9, 2018): 1146–51. https://doi.org/10.1126/science.aap9559.

Waltzman, Rand. "The Weaponization of Information: The Need for Cognitive Security." RAND Corporation, April 27, 2017. https://www.rand.org/pubs/testimonies/CT473.html.

Wardle, Claire. "Misinformation Has Created a New World Disorder." Scientific American. Accessed May 21, 2022. https://doi.org/10.1038/scientificamerican0919-88.

West, Darrell M. "How to Combat Fake News and Disinformation." *Brookings* (blog), December 18, 2017. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

Whaley, Barton. "Toward a General Theory of Deception." *Journal of Strategic Studies* 5, no. 1 (March 1, 1982): 178–92. https://doi.org/10.1080/01402398208437106.

Whitton, John B. Review of *Review of International Propaganda. Its Legal and Diplomatic Control*, by L. John Martin. *Harvard Law Review* 72, no. 2 (1958): 396–400. https://doi.org/10.2307/1338178.

Willis, Mikki. "Plandemic," May 2020. https://plandemicseries.com/.

Wilson, Tom, Kaitlyn Zhou, and Kate Starbird. "Assembling Strategic Narratives: Information Operations as Collaborative Work within an Online Community." *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (November 2018): 1–26. https://doi.org/10.1145/3274452.

Wolff, Greg G. "Influenza Vaccination and Respiratory Virus Interference Among Department of Defense Personnel During the 2017–2018 Influenza Season." *Vaccine* 38, no. 2 (January 10, 2020): 350–54. https://doi.org/10.1016/j.vaccine.2019.10.005.

Yancey-Bragg, N'dea, and Joel Shannon. "Claim in Viral 'Plandemic' Video 'Could Lead to Imminent Harm,' Facebook Says." *USA TODAY*, May 9, 2020. https://www.usatoday.com/story/tech/2020/05/08/facebook-plandemic-judy-mikovits-shares-false-coronavirus-info/3095471001/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California