NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEFENDING AMERICAN DEMOCRACY IN THE POST-TRUTH AGE: A ROADMAP TO A WHOLE-OF-SOCIETY APPROACH

by

Katelyn M. Mason

September 2020

Co-Advisors: Christopher Bellavita (contractor)
Rodrigo Nieto-Gomez

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2020	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE DEFENDING AMERICAN DEMOCRACY IN THE POST-TRUTH AGE: A ROADMAP TO A WHOLE-OF-SOCIETY APPROACH	5. FUNDING NUMBERS
6. AUTHOR(S) Katelyn M. Mason	
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)

False narratives increasingly threaten U.S. democratic society and evolving adversaries and technology are making it more difficult for authorities and the public to differentiate between fact, opinion, and falsehoods. Despite experts proposing a variety of recommendations to mitigate this threat, the United States does not have a national-level strategy in place to combat deceptive messaging in a comprehensive and coordinated manner. The author analyzed over 170 recommendations for a U.S. strategy and found that many of them hinge on broad coordination between all U.S. stakeholders, which includes, but is not limited to, all levels of government, private sector, academia, media, and civil society. To identify how the United States can achieve the coordination needed to combat deceptive messaging, the author conducted a case study of the role of coordination in the European Union (EU) response to disinformation and an assessment of collective impact, a cross-sector coordination method used for complex social problems, for use in the United States. The conclusions of the case study and assessment endorse U.S. government practitioners to use collective impact and components of existing practices in the EU response to disinformation to build a coordinated national strategy to challenge those who wish to harm American democracy and U.S. interests via cyber-based deceptive messaging.

14. SUBJECT TERMS disinformation, deceptive messaging, post-truth, falsehoods, coordination, collective impact, foreign influence, government strategy, fake news, propaganda, whole-of-society, deepfake, European Union, EU	15. NUMBER OF PAGES 129
	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.

DEFENDING AMERICAN DEMOCRACY IN THE POST-TRUTH AGE: A ROADMAP TO A WHOLE-OF-SOCIETY APPROACH

Katelyn M. Mason
Lead Intelligence Analyst, Northern California Regional Intelligence Center
B, Tiffin University, 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
September 2020

Approved by: Christopher Bellavita
Co-Advisor

Rodrigo Nieto-Gomez
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

False narratives increasingly threaten U.S. democratic society and evolving adversaries and technology are making it more difficult for authorities and the public to differentiate between fact, opinion, and falsehoods. Despite experts proposing a variety of recommendations to mitigate this threat, the United States does not have a national-level strategy in place to combat deceptive messaging in a comprehensive and coordinated manner. The author analyzed over 170 recommendations for a U.S. strategy and found that many of them hinge on broad coordination between all U.S. stakeholders, which includes, but is not limited to, all levels of government, private sector, academia, media, and civil society. To identify how the United States can achieve the coordination needed to combat deceptive messaging, the author conducted a case study of the role of coordination in the European Union (EU) response to disinformation and an assessment of collective impact, a cross-sector coordination method used for complex social problems, for use in the United States. The conclusions of the case study and assessment endorse U.S. government practitioners to use collective impact and components of existing practices in the EU response to disinformation to build a coordinated national strategy to challenge those who wish to harm American democracy and U.S. interests via cyber-based deceptive messaging.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. DECEPTIVE MESSAGING IN THE UNITED STATES 1
- A. RESEARCH QUESTION 1
- B. PROBLEM STATEMENT 1
- C. RESEARCH DESIGN 6
- D. LITERATURE REVIEW: BARRIERS TO ADOPTION AND IMPLEMENTATION 9
  - 1. The Complex, Ambiguous, and Evolving Threat Picture 10
  - 2. Accountability and Leadership 15

II. THE U.S. RESPONSE STRATEGY PLAYBOOK 21
- A. PUBLIC RESILIENCE 22
  - 1. Government Transparency 23
  - 2. Awareness Campaigns 26
  - 3. Media Literacy 28
- B. COORDINATION 32

III. GOVERNMENT COORDINATION IN PRACTICE 41
- A. THE EUROPEAN UNION'S JOINT AND COORDINATED ACTION AGAINST DISINFORMATION 42
- B. LESSONS LEARNED AND SMART PRACTICES 48

IV. COLLECTIVE IMPACT: A ROADMAP FOR COORDINATION 53
- A. THE CONDITIONS OF IMPACT 54
- B. ASSESSMENT FOR APPLICABILITY 62

V. MOBILIZING FOR SYNERGY 71
- A. RECOMMENDATIONS 71
- B. CONCLUSIONS 78

APPENDIX A. THE WAR ON PINEAPPLE 81

APPENDIX B. GLOSSARY OF TERMS 83

LIST OF REFERENCES 87

INITIAL DISTRIBUTION LIST 103

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Overview of EU Joint and Coordinated Action against Disinformation. 45

Figure 2. The Phases of Collective Impact.....58

Figure 3. Collective Impact Feasibility Framework.....64

Figure 4. The War on Pineapple and Understanding Foreign Interference.....81

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Coordination Terminology.....37

Table 2. The Five Conditions of Collective Impact.....56

Table 3. Public Policies that Encourage Collective Impact.....61

Table 4. U.S. Government Agencies Fighting Deceptive Messaging. 77

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
AMWG	Active Measures Working Group
ASD	Alliance for Securing Democracy
CFITF	Countering Foreign Influence Task Force
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Department of State
DOT	Department of Treasury
DRA	Deepfake Reports Act
EEAS	European External Action Service
EU	European Union
EUCOM	U.S. European Command
FBI	Federal Bureau of Investigation
FITF	Foreign Influence Task Force
FSLTT	federal, state, local, tribal, and territorial
G7	Group of Seven
GEC	Global Engagement Center
HSAC	Homeland Security Advisory Council
HSIN	Homeland Security Information Network
IoT	Internet of Things
ML	media literacy
NATO	North Atlantic Treaty Organization
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center
NGO	non-governmental organizations
NSA	National Security Agency
NYS	New York State

ODNI	Office of the Director of National Intelligence
RIG	Russian Influence Group
SBA	Small Business Administration
SOCOM	U.S. Special Operations Command
SPAC	strategic planning action committee
USAGM	U.S. Agency for Global Media
USAID	U.S. Agency for International Development
USCYBERCOM	U.S. Cyber Command
USDOJ	U.S. Department of Justice

EXECUTIVE SUMMARY

The use of deception and propaganda is weaved throughout human history and war, yet in recent years, these manipulative actions have become a renewed concern for national security efforts around the world.[1] Falsehoods that travel through cyber-based platforms can exponentially reach more people in less time and can manifest into dangerous physical-world outcomes. Cyber-based falsehoods have inflamed societal tensions, stimulated escalations to violence, affected economies and business, breached election security, misallocated resources during terror attacks or natural disasters, contributed to a rise in deadly but preventable diseases, and facilitated major geopolitical objectives.[2] Furthermore, adversaries and technology are evolving, which makes it more difficult for authorities and the public to differentiate between fact, opinion, and falsehoods.

While many notable deceptive messaging campaigns can be attributed to Russian-backed sources, other state and non-state actors with geopolitical, ideological, political, monetary, or notoriety-driven motivations increasingly use this tactic.[3] In comparison to the extensive and growing threat, efforts in the United States to combat deceptive

---

[1] Char Sample, Connie Justice, and Emily Darraj, "A Model for Evaluating Fake News" (paper presented at the CyCon U.S. 2018, Washington, DC, November 14–15, 2018), 1–2, https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session4-Paper1.pdf?ver=2018-11-13-160900-603.

[2] Samantha M. Korta, "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security" (master's thesis, Naval Postgraduate School, 2018), 1–10, http://hdl.handle.net/10945/58322; Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–1151, http://www.sciencemag.org/lookup/doi/10.1126/science.aap9559; Gjorgji Veljovski, Nenad Taneski, and Metodija Dojchinovski, "The Danger of 'Hybrid Warfare' from a Sophisticated Adversary: The Russian 'Hybridity' in the Ukrainian Conflict," *Defense & Security Analysis* 33, no. 4 (2017): 292–307, https://doi.org/10.1080/14751798.2017.1377883.

[3] Christina Nemr and William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Washington, DC: Park Advisors, 2019), 20–24, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

messaging are disproportionate and insufficient.[4] To improve societal resilience in America scholars and practitioners have developed a broad spectrum of strategies that the U.S. government could use to mitigate the threat; however, many have yet to be adopted and implemented. To improve response efforts, this research answers the following question: Which defensive strategies should the United States prioritize to mitigate the impact of deceptive messaging, and how can government leaders implement them?

To answer the research question, I collected a sample of 170 deceptive messaging related recommendations from a variety of subject matter experts. This study primarily focuses on defensive measures to help close the vulnerabilities of U.S. society, rather than strategies that aim to target, censor, or counter influence audiences. Using thematic analysis, the recommendations were categorized into five themes: (1) public resilience, (2) policy and regulation, (3) coordination, (4) research and development, and (5) operational activities. Out of the five themes, a majority of the recommendations primarily fell under two categories, (1) public resilience, and (2) coordination. Upon further exploration of the recommendations within public resilience and coordination, it was clear that many of the recommendations within other categories relied on close collaboration with stakeholders from a variety of disciplines, often referred to as a whole-of-nation or whole-of-society

[4] Daniel Coats, *2018 Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2018), 4–27, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf; Daniel Coats, *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), 5–7, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; Samantha Bradshaw and Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation* (Oxford, UK: Oxford Internet Institute's Computational Propaganda Research Project, 2018), 5, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf; Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee* (Washington, DC: Department of Homeland Security, 2019), 10, https://www.dhs.gov/sites/default/files/publications/ope/hsac/19_0521_final-interim-report-of-countering-foreign-influence-subcommittee.pdf.

approach.[5] The importance of coordination influenced the rest of this research to focus on identifying methods that U.S. government leaders can use to create a whole-of-society approach to mitigate deceptive messaging through a case study of the European Union (EU) response to disinformation and an assessment of collective impact, a cross-sector coordination method often used for complex social problems.

A review of the literature revealed two themes that present a hindrance to the coordination needed for a whole-of-society approach in the United States, the lack of a common understanding of the complex, ambiguous, and evolving nature of the threat, and a lack of clearly defined responsibilities and leadership among the stakeholders that could or should play a role in responding to the threat. To help simplify the terminology used to describe the threat, I use the term deceptive messaging in this thesis as a comprehensive phrase to capture the types of information used throughout the literature to define the threat. Despite the complexity, ambiguity, and lack of the leadership, the consensus across experts for a government-led multi-stakeholder approach has grown in popularity in dominant literature.[6] The growing support among scholars for the government to take a leadership role and the documented tasking of the Department of Homeland Security (DHS) to become the leading entity to establish a national strategy to counter foreign influence and

---

[5] Rand Waltzman, *The Weaponization of Information: The Need for Cognitive Security*, CT-473 (Santa Monica, CA: RAND, 2017), 4–5, http://www.rand.org/pubs/testimonies/CT473.html; Jamie Fly, Laura Rosenberger, and David Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies* (Washington, DC: The German Marshall Fund of the United States, 2018), 17–22, http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies; Mark Warner, "A New Doctrine for Cyberwarfare & Information Operations" (speech, Center for a New American Security, December 7, 2019), https://www.warner.senate.gov/public/index.cfm/2018/12/warner-calls-for-society.

[6] Dipayan Ghosh and Ben Scott, *#DigitalDeceit: The Technologies behind Precision Propaganda on the Internet* (Washington, DC: New America, 2018), 4, https://d1y8sb8igg2f8e.cloudfront.net/documents/digital-deceit-final-v3.pdf; Daniel Fried and Alina Polyakova, *Democratic Defense against Disinformation* (Washington, DC: Atlantic Council, 2018), 10–14, http://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_FINAL.pdf; Sijbren de Jong et al., *Inside the Kremlin House of Mirrors: How Liberal Democracies Can Counter Russian Disinformation and Societal Interference* (The Hague, Netherlands: The Hague Centre for Strategic Studies, 2017), 2, https://hcss.nl/report/inside-kremlin-house-mirrors-how-liberal-democracies-can-counter-russian-disinformation-0.

ensure effective coordination are promising steps toward overcoming the obstacles to building a collective response to deceptive messaging.[7]

In addition to these positive steps, the U.S. government can leverage the strengths and weaknesses of existing disinformation response efforts around the world to accelerate progress. The case study of the EU's fight against disinformation identified many coordination strategies the United States can leverage, such as the East StratCom Task Force, the *EU Code of Practice on Disinformation*, and the Rapid Alert System.[8] Other smart practices from the EU response to disinformation included the top-down driven strategy development, the availability and accessibility of information about the threat and response efforts, and the emphasis on citizen engagement.[9] The EU case study provides valuable insight into building effective cross-sector coordination in its response to disinformation; however, it does not explicitly identify the steps that must be taken to build a connected network of stakeholders with a variety of missions, budgets, goals, and expectations.

Collective impact is one method, with proven success, that can serve as a roadmap for the U.S. government to build a whole-of-society approach to combat deceptive messaging. Collective impact initiatives are defined as, "long-term commitments by a group of important actors from different sectors to a common agenda for solving a specific social problem."[10] Initiatives are structured around five conditions: (1) common agenda,

---

[7] Homeland Security Advisory Council, *Countering Foreign Influence Subcommittee, Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*, 10.

[8] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the Implementation of the Action Plan against Disinformation* (Brussels: European Commission, 2019), 1–10, https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf; European Union External Action, *Rapid Alert System Strengthening Coordinated and Joint Responses to Disinformation* (Brussels: European Union External Action, 2019), 1, https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.

[9] European Commission, *Joint Communication...Report on the Implementation of the Action Plan against Disinformation*.

[10] John Kania and Mark Kramer, "Collective Impact," *Stanford Social Innovation Review* 9, no. 1 (Winter 2011): 39, https://ssir.org/articles/entry/collective_impact.

(2) shared measurement, (3) mutually reinforcing activities, (4) continuous communication, and (5) backbone support, all of which are aimed to align the efforts and maximize the resources of a diverse group of stakeholders.[11] Such initiatives have been well studied and practitioners can leverage the abundance of resources and tools, such as the five phases of collective impact, public policies that encourage collective impact, and the collective impact feasibility framework, which provide specific action items and key milestones to foster successful initiatives.[12] Based on the alignment with coordination needs, the expected outcome of an assessment using the feasibility framework, the measurable success in many cases and noticeable traces of elements in the EU response to disinformation, collective impact is a method that should be strongly considered for adoption in the United States.

A national strategy to combat deceptive messaging must establish robust coordination across sectors as a priority, and once an entity is charged with the responsibility to lead this effort, practitioners can assess the collective impact method for use, and employ smart practices from the EU response to disinformation to accelerate progress toward achieving the level of coordination needed. Establishing effective coordination and domain awareness is just the first step in building a comprehensive national strategy to mitigate deceptive messaging in the United States. In addition to identifying and convening relevant government and non-government stakeholders, additional research is needed on the other types of expert recommendations identified in this thesis (public resilience, policy and regulation, research and development, and operational activities), media literacy training for all government employees to detect and verify information, strategic communication and information marketing, and existing

---

[11] Kania and Kramer, "Collective Impact," 41.

[12] Tamarack Institute, *Collective Impact Self-Assessment and Planning Tool* (Waterloo, ON: Tamarack Institute, 2017), 1–12, https://www.tamarackcommunity.ca/hubfs/Collective%20Impact/Tools/CI%20Self%20Assessment%20Tool.pdf?hsCtaTracking=8df74891-21af-4a7c-88d7-bb024f0d7d62%7C90f5999e-f7d9-4112-890e-96ed8a56a460; Thaddeus Ferber and Erin White, "Making Public Policy Collective Impact Friendly," *Stanford Innovation Review* 12, no. 4 (Fall 2014): 23, https://ssir.org/pdf/Fall_2014_Making_Public_Policy_Collective_Impact_Friendly.pdf; FSG, *Collective Impact Feasibility Framework* (Boston: FSG, 2015), 3, https://www.collectiveimpactforum.org/sites/default/files/Collective%20Impact%20Feasibility%20Framework.pdf.

practices, systems, and knowledge, such as the National Network of Fusion Centers and the DHS Homeland Security Information Network (HSIN), which can possibly be leveraged to use for combatting deceptive messaging in America.

Deceptive messaging campaigns are only expected to become more pervasive and more difficult to detect, track, and attribute with the adversary adapting to countermeasures and policies, and the evolution of technology, such as deepfakes and encryption. The lack of visibility or inability to identify deceptive messaging will make information sharing, collaboration, and public engagement even more important. Should the U.S. government not take the necessary steps to bring together important parts of society to challenge those who wish to harm the United States via cyber-based deceptive messaging, it may be on a path in which fake news-induced catastrophes are reality.

ACKNOWLEDGMENTS

This endeavor has been both a significant challenge and accomplishment thus far in my life, and I could have not done it without the support of many great people. They say it takes a village to raise a child, and I think the same applies for a graduate student. I am so grateful for the village that guided me through this process, and I would like to personally recognize and thank them for their support.

First and foremost, to my management team, your unwavering support and nomination to this program afforded me many opportunities that will last a lifetime. To Dylan McCulley and my team, your willingness to step up and often take on extra work in my absence did not go unnoticed, and I will forever be indebted for your leadership, teamwork, dedication, and understanding.

I would also like to recognize and thank the many people at the Center for Homeland Defense and Security. To the class of 1801/1802, I am inspired by your work ethic and dedication to serve your city, county, state, and country. I am grateful for your mentorship, advice, and most importantly, your friendship. I am especially grateful to Jason Lyon and Harley Lenart for always keeping me focused and extending their help whenever needed. To my advisors, Rodrigo and Chris, and the amazing support staff, Noel and Greta, thank you for guiding me through this difficult process and dedicating your time and expertise to ensure my work was the best that it could be. Finally, to Sam Korta, I appreciate that you provided me with inspiration for my thesis and became a great friend and colleague throughout the process. You have all changed my life in so many ways, and for that, I thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

PROLOGUE: FAKE NEWS-INDUCED NUCLEAR WAR

Citizens of the world live at a time when government and world leaders can and often communicate with each other and constituents quickly through the internet. This societal trend bears many great benefits, but also significant dangers. The average person "with relatively modest amounts of data and computing power" can create videos of anyone saying anything.[13] Potential victims of such manipulation include a local police chief, a city mayor, a state's governor, military personnel, a medical professional, all the way up to the President and Commander in Chief. The ability for someone to manipulate the words of individuals of power has the potential to create a catastrophe that would be difficult to prevent or reverse.

The internet ecosystem allows users to create and share information rapidly and anonymously regardless of the quality or accuracy. Imagine a video of your local police chief making derogatory or racist remarks, that were never actually made, being posted online, and the resulting public outcry and damage to the community's trust that would ensue. This example is just one hypothetical scenario, and the narratives that can be created from manipulating information are practically endless. Research has shown that counter messaging with the correct information is not exactly an effective method to reverse disinformation because of humans' natural tendency not to change their minds with the introduction of new or different information.[14] Public trust in government is fragile, and once a disinformation campaign goes viral, it can manifest as real physical threats to society that cannot be stopped.

The physical threats that can manifest from online disinformation campaigns can be, and have been, as significant as bringing two nations to the brink of nuclear war. In 2016, an online news story reported that the Israeli defense minister threatened Pakistan

---

[13] Shruti Agarwal et al., "Protecting World Leaders Against Deep Fakes," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops* (June 2019): 38–45, https://farid.berkeley.edu/downloads/publications/cvpr19/cvpr19a.pdf.

[14] Nemr and Gangware, *Weapons of Mass Distraction*, 11.

with a nuclear attack.[15] Despite the story being quickly debunked, this perceived threat from Israel prompted the Pakistani defense minister to respond via Twitter to remind Israel that Pakistan was a nuclear state.[16] Luckily, the incident was resolved quickly with swift corrective measures from the Israeli government and social media users who learned that the article was false.[17]

Since 2016, fake news stories have become more pervasive and realistic, making it more difficult to distinguish between real, fabricated, or framed information. If a false narrative or deepfake video of the President of the United States making derogatory statements about another country or state-actor were to spread through the internet, perhaps reaching real political leaders or activist groups, the country could be driven to the brink of a nuclear conflict as with Pakistan and Israel. Are United States' leaders prepared to defend its society and democracy from fake news-induced catastrophes?

---

[15] Russell Goldman, "Reading Fake News, Pakistani Minister Directs Nuclear Threat at Israel," *New York Times*, December 24, 2016, https://www.nytimes.com/2016/12/24/world/asia/pakistan-israel-khawaja-asif-fake-news-nuclear.html.

[16] Goldman.

[17] Goldman.

I. DECEPTIVE MESSAGING IN THE UNITED STATES

All war is based on deception.

~Sun Tzu[1]

A. RESEARCH QUESTION

This research answers the following question: Which defensive strategies should the United States prioritize to mitigate the impact of deceptive messaging, and how can government leaders implement them?

B. PROBLEM STATEMENT

The use of deception and propaganda is weaved throughout human history and war and can be traced back as far as the Neolithic age.[2] Yet in recent years, these manipulative actions have become a renewed concern for national security efforts around the world because falsehoods now travel through cyber-based mediums, such as social media, in which they can exponentially reach more people in less time. In fact, a study in 2018 found that false news spreads further, faster, deeper, and more broadly than the truth.[3]

Furthermore, deceptive information thrives in liberal democracies because it blends in with legitimate discourse under the protections of free speech.[4] The quick delivery of

---

[1] Sun Tzu, *The Art of War* (Greyhound Press, 2017), 4.

[2] Char Sample, Connie Justice, and Emily Darraj, "A Model for Evaluating Fake News" (paper presented at the CyCon U.S. 2018 Washington, DC, November 14–15, 2018), 1–2, https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session4-Paper1.pdf?ver=2018-11-13-160900-603.

[3] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1147, http://www.sciencemag.org/lookup/doi/10.1126/science.aap9559.

[4] Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency* (Scottsdale, AZ: New Foundation Organization, 2018), 99, https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf; Insikt Group, *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion* (Somerville, MA: Recorded Future, 2019), 14, https://www.recordedfuture.com/china-social-media-operations/.

information to the masses who are unable to differentiate between legitimate or deceptive information has reinvigorated the value and power of this age-old war tactic, which makes it a new world threat.

The physical-world outcomes that manifest from cyber-based falsehoods are dangerous. Researchers have found that deceptive messaging campaigns have inflamed societal tensions, stimulated escalations to violence, affected economies and business, breached election security, misallocated resources during terror attacks or natural disasters, contributed to a rise in deadly but preventable diseases, and facilitated major geopolitical objectives.[5] Since the government has an expectation to protect the public from such threats, each of these outcomes contributes to a gradual decay in the public's trust in government and democratic institutions. Yuval Harari says, "underneath all the fake news, there are real facts and real suffering."[6] Anyone in the world with minimal effort and access to technology can anonymously inflict such outcomes on any community at any time, which makes the dangers of this threat even more concerning.

Deceptive messaging campaigns are being weaponized all over the world for various objectives. The most notable cases of deceptive messaging campaigns with significant physical impacts include Russia's use of "misdirection, misinformation, and propaganda" to facilitate the annexation of Crimea in 2014, the spread of false information that contributed to an anti-vaccination movement and subsequent measles outbreaks around the world, and the Russian influence operations that interfered with the 2016 U.S. presidential elections.[7] More recent examples include efforts to "discredit the pro-

---

[5] Samantha M. Korta, "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security" (master's thesis, Naval Postgraduate School, 2018), 1–10, http://hdl.handle.net/10945/58322; Vosoughi, Roy, and Aral, "The Spread of True and False News Online," 1146–1151; Gjorgji Veljovski, Nenad Taneski, and Metodija Dojchinovski, "The Danger of 'Hybrid Warfare' from a Sophisticated Adversary: The Russian 'Hybridity' in the Ukrainian Conflict," *Defense & Security Analysis* 33, no. 4 (2017): 292–307, https://doi.org/10.1080/14751798.2017.1377883.

[6] Yuval Harari, *21 Lessons for the 21st Century* (New York: Penguin Random House LLC, 2018), 247.

[7] Veljovski, Taneski, and Dojchinovski, "The Danger of 'Hybrid Warfare' from a Sophisticated Adversary," 304; Korta, "Fake News, Conspiracy Theories, and Lies," 1; Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, 2019), 1, https://www.justice.gov/storage/report.pdf.

democracy movement" in Hong Kong in 2019, and efforts to target major 2020 democratic elections.[8] The global nature of the threat is not only targeting American's but also American interests around the world.

While many notable deceptive messaging campaigns can be attributed to Russian-backed sources, this tactic can be employed by other nations to promote geopolitical objectives. Other nations known to use deceptive messaging tactics online include China, Iran, and North Korea.[9] For example, in 2018, a cyber-security company found that Iranian-backed networks of "inauthentic news sites and social media accounts," some posing as Americans, targeted worldwide audiences to promote Iranian political interests.[10] The minimal cost and resources needed for disinformation campaigns online compared to traditional military tactics make it an attractive option for a nation to achieve its objectives.

The low threshold of resources needed for a disinformation campaign also makes it an attractive tactic to non-state actors, domestic and abroad. Non-state actors may be motivated by ideology, political desires, monetary benefits, or notoriety. For example, alt-right groups have spread "fake news stories, conspiracy theories, and memes virally on digital platforms" aimed at elections.[11] Other non-state actors with less malicious intentions use deceptive messaging to exploit pay-per-click advertising online and

---

[8] Sam Alexander et al., *Combatting Targeted Disinformation Campaigns: A Whole-of-Society-Issue* (Washington, DC: Department of Homeland Security, 2019), 20–21, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf; Nathaniel Gleicher, "How we respond to inauthentic behavior on our platforms: Policy update," Facebook, October 21, 2019, https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/.

[9] Christina Nemr and William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Washington, DC: Park Advisors, 2019), 20–24, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

[10] FireEye, *Suspected Iranian Influence Operation: Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences* (Milpitas, CA: FireEye, 2018), 1–16, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf.

[11] Judit Bayer et al., *Disinformation and Propaganda—Impact on the Functioning of the Rule of Law in the EU and Its Member States* (Brussels: European Union, Policy Department for Citizens' Rights and Constitutional Affairs, 2019), 40, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

maximize clicks on ads that redirect users and ultimately generate profits.[12] Regardless of motivation, non-state actors further complicate the information space with a large volume of false information.

The rapid diffusion of deceptive content relies on a third group of actors who create or share it unintentionally. Unwitting internet users initiate and facilitate the spread of false narratives because they believe the information is either true or simply do not know if it is incorrect. In 1984, Yuri Bezmenov, a former PGU KGB informant, noted that Soviet active measures were so successful because "most if it [demoralization] is done by Americans doing it to other Americans."[13] With an estimated 3.9 billion internet users today, the threat of deceptive messaging extends beyond geographical regions and is not attributable to just foreign competitors.[14]

Efforts in the United States to combat deceptive messaging are disproportionate to the extensive and growing threat. The Office of the Director of National Intelligence (ODNI) identified influence operations using social media as a significant threat to the country in the 2018 and 2019 *World Wide Threat Assessment*, and evidence suggests it is only growing.[15] Yet, the Countering Foreign Influence Subcommittee wrote in a 2019 report that no agency or entity has been mandated to lead efforts to counter foreign influence, and as of May 2019, "the United States has no national strategy to counter

---

[12] Canadian Security Intelligence Service, *Who Said What?: The Security Challenges of Modern Disinformation* (Ottawa, ON: Canadian Security Intelligence Service, 2018), 99–104, https://www.canada.ca/en/security-intelligence-service/corporate/publications/who-said-what-the-security-challenges-of-modern-disinformation.html.

[13] "Soviet Subversion of the Free World Press," April 24, 2011, Thomas Andrews, YouTube, video, 1:21:28, https://www.youtube.com/watch?v=Cnf0I2dQ0i0.

[14] "Statistics," International Telecommunications Union, accessed August 6, 2019, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[15] Daniel Coats, *2018 Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2018), 4–27, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf; Daniel Coats, *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), 5–7, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; Samantha Bradshaw and Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation* (Oxford, UK: Oxford Internet Institute's Computational Propaganda Research Project, 2018), 5, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

foreign influence."[16] Additionally, Nina Jankowicz, a Global Fellow at the Kennan Institute, pointed out that the dedication of resources to combat disinformation and malign influence are nominal.[17] In a 2019 Congressional hearing, she stated, "The planned budget for RT [Russian international television network]... and certainly only a small part of the overall Russian disinformation ecosystem—is $277 million in 2020."[18] The Global Engagement Center (GEC), the designated agency to lead the U.S. government efforts to counter propaganda and disinformation, base budget request for FY19 was just $53 million.[19] The United States has not yet put forth adequate resources nor a national strategy to fight deceptive messaging and foreign influence.

Although other U.S. government agencies have begun to dedicate resources to the deceptive messaging threat, no overarching and comprehensive strategy currently exists to bridge those response efforts. Elizabeth Bodine-Baron et al. emphasized, "Without cooperation and coordination, efforts will remain piecemeal and inadequate, and the United States will remain vulnerable to influence campaigns by Russia and other adversaries."[20] A strongly coordinated response effort and strategy to unify government agencies, the private sector, and civil society could generate resources more proportional to the deceptive messaging threat.

To improve the United States' response to deceptive messaging, scholars and practitioners have developed a broad spectrum of strategies that the U.S. government could

---

[16] Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee* (Washington, DC: Department of Homeland Security, 2019), 10, https://www.dhs.gov/sites/default/files/publications/ope/hsac/19_0521_final-interim-report-of-countering-foreign-influence-subcommittee.pdf.

[17] *Statement of Nina Jankowicz Woodrow Wilson International Center for Scholars, Kennan Institute before the United States House Committee on Appropriations Subcommittee on State, Foreign Operations, and Related Programs concerning "United States Efforts to Counter Russian Disinformation and Malign Influence,"* House of Representatives, 116th Cong., 1st sess., July 10, 2019, 1, https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-JankowiczN-20190710.pdf.

[18] H.R., *Statement of Nina Jankowicz*, 3.

[19] "Global Engagement Center," Department of State, accessed February 8, 2019, https://www.state.gov/r/gec/.

[20] Elizabeth Bodine-Baron et al., *Countering Russian Social Media Influence* (Santa Monica, CA: RAND, 2018), xiii, https://doi.org/10.7249/RR2740.

adopt to mitigate the threat. However, many of these strategies have yet to be implemented. Therefore, the purpose of this study is to compile and examine the plethora of recommended strategies, determine which of those are the most critical to implement, and identify how the nation's leaders can begin executing them. This study primarily focuses on defensive measures to help close the vulnerabilities of U.S. society, rather than strategies that aim to target, censor, or counter influence audiences. Deceptive messaging cannot be solved, but the U.S. government can do much to mitigate it.

C. RESEARCH DESIGN

Rather than proposing additional prescriptions, this thesis aims to understand better the strategy recommendations that exist to mitigate deceptive messaging and how the U.S. government may be able to implement them. To address this topic, I collected a sample of 170 deceptive messaging related recommendations from think tanks, academics and scholars, a security advocacy group, research institutes, private sector consulting companies, and government practitioners. The collection of prescriptions focused on defensive measures for U.S. society that aimed to protect the domestic population or U.S. interests, rather than offensive measures targeting other populations.

To understand the collected sample best, I conducted a thematic analysis of the open-source prescriptions. Lorelli Nowell et al. argue that thematic analysis is a "useful method for examining the perspectives of different research participants, highlighting similarities and differences, and generating unanticipated insights."[21] The identification of commonalities and differences among experts will be valuable to help identify where U.S. government leaders can make the greatest impact and be most efficient in the development and implementation of response efforts.

The method is divided in six steps. Nowell et al. defines those steps as: "(1) familiarizing yourself with your data, (2) generating initial codes, (3) searching for themes,

---

[21] Lorelli S. Nowell et al., Thematic Analysis: Striving to Meet the Trustworthiness Criteria," *International Journal of Qualitative Methods* 16, no. 1 (2017): 1–13, https://doi.org/10.1177/1609406917733847.

(4) reviewing themes, (5) defining and naming themes, and (6) producing the report,"[22] Therefore, I first sorted the prescriptions into five themes. Sorting the prescriptions into apparent themes provides flexibility; however, it also means this task is relatively subjective, which may potentially lead to inconsistencies in the organization of the data when repeated by someone else.[23] To account for this challenge, I coded the data that could be interpreted to support more than one theme with a secondary code when applicable. The secondary themes for prescriptions provided additional insight into how the themes could potentially be interpreted differently by other people.

The five themes identified across the dataset were: (1) public resilience, (2) policy and regulation, (3) coordination, (4) research and development, and (5) operational activities. A statistical review of each theme revealed that public resilience and coordination related recommendations accounted for nearly half of all the recommendations in the sample. Due to time and resource limitations, the rest of the research in this thesis focused on further exploration of those two categories due to being overwhelmingly popular among experts.

A detailed qualitative review of the public resilience and coordination themes revealed that coordination appeared to be a common sub-component for the prescriptions within the other themes. The recommendations within other themes used language, such as "partnership," "collaborate," "assist," and "coordinate," as descriptors. The centrality of coordination as a standalone theme and sub-component to other themes influenced the rest of this research to focus on identifying methods U.S. government leaders could use to implement organized coordination and engagement between relevant stakeholders through a case study and an assessment of a well-studied and well-practiced multi-sector coordination method used in the public sector.

The case study examines and explains how coordination efforts play a role in the European Union's (EU) response to disinformation. This method was chosen because

---

[22] Nowell et al., 4.

[23] Nowell et al., 2.

responses to deceptive messaging are complex and so new that studies about them are limited to the minimal amounts of data available. Henry Harder states that explanatory case studies are useful for "investigating and explaining complex phenomena that may not lend themselves easily to quantitative research methodologies."[24] Despite not being able to quantify coordination efforts or determine their true effectiveness, the available qualitative data about the EU response is useful to understand the importance of coordination better and how it can be accomplished for deceptive messaging response efforts. It will also help identify potential strengths and weaknesses of the EU's model and potential applicability for replication in the United States.

The EU response to disinformation was selected as a case study based on three primary criteria: (1) experts hold the EU's response in high regard as a leader in addressing deceptive messaging, (2) it is comprised of liberal democracies with many similar qualities to the United States, and (3) its response has been developing for over four years and thus provides more data points to evaluate.[25] I collected data for the case study from reports and press releases published by EU institutions, reports from two different think tanks, and expert testimony from a U.S. Congressional hearing. Since deceptive messaging is an emerging issue, the EU presents an opportunity for other countries to consider mirroring its approach, or elements of it, as a possible option for securing their own populations. The single case study has limitations because fewer data points are available as opposed to a multi-case study nor does it explain a detailed methodology of how coordination can be achieved. Additional case studies were considered for this thesis; however, the availability of data and time restraints resulted in just a single case study.

To account for the limitations of the EU case study, this thesis also provides an assessment of collective impact, a methodology for multi-sector coordination. This method

---

[24] Henry Harder, "Explanatory Case Study," in *Encyclopedia of Case Study Research*, ed. Albert Mills, Gabrielle Durepos and Elden Wiebe (Thousand Oaks: SAGE Publications Inc., 2012), 371–375, https://dx.doi.org/10.4135/9781412957397.

[25] Alina Polyakova and Daniel Fried, "Europe Is Starting to Tackle Disinformation. The U.S. Is Lagging," *Washington Post*, June 17, 2019, https://www.washingtonpost.com/opinions/2019/06/17/europe-is-starting-tackle-disinformation-us-is-lagging/; "Tackling Online Disinformation," European Commission, last modified June 17, 2019, https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation.

was primarily chosen for assessment because its framework aligns with many of the coordination needs identified by expert recommendations for a response to deceptive messaging in the United States. The assessment of this method first describes collective impact, and then examines its feasibility, benefits, use cases, limitations, and how it can be applied to the deceptive messaging problem. The combined use of thematic analysis, explanatory case study, and assessment of collective impact in this thesis offers multiple perspectives and options for the U.S. government to consider for improving government coordination in a meaningful way to mitigate deceptive messaging.

D. LITERATURE REVIEW: BARRIERS TO ADOPTION AND IMPLEMENTATION

This chapter examines two themes within the literature that present a hindrance to deceptive messaging response efforts in the United States. The first theme is the lack of a common understanding of the complex, ambiguous, and evolving nature of the threat. Jamie Fly, Laura Rosenberger, and David Salvo assert that the slow response from the U.S. government after Russian influence was detected was partly due to a lack of understanding the scope of the campaign.[26] Additionally, Annina Claesson points out that the United States views the deceptive messaging threat "narrowly as the dissemination of 'fake news' by Russian trolls" in contrast to "a problem rooted in complex and rapid socioeconomic changes."[27] Although it is common for researchers to disagree on how to define phenomena, the way in which the deceptive messaging threat is defined or described throughout the literature is exceptionally scattered and detracts from solution- or action-focused discussions.

The research that aims to provide a better understanding of the threat uses a plethora of terminology and frameworks to describe it, which has created additional confusion in

---

[26] Jamie Fly, Laura Rosenberger, and David Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies* (Washington, DC: The German Marshall Fund of the United States, 2018), 11, http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

[27] Annina Claesson, "Coming Together to Fight Fake News: Lessons from the European Approach to Disinformation," *New Perspectives in Foreign Policy*, no. 17 (Spring 2019): 13–19, https://www.csis.org/coming-together-fight-fake-news-lessons-european-approach-disinformation.

the discourse. Therefore, to help simplify the terminology used to describe the threat, I use the term deceptive messaging in this thesis as a comprehensive phrase to capture the types of information used throughout the literature to define the threat. Such terms include fake news, propaganda, disinformation, misinformation, and mal-information.

The second theme is a lack of clearly defined responsibilities and leadership among the stakeholders that could or should play a role in responding to deceptive messaging. Supporting Elizabeth Bodine-Baron et al.'s argument for the need of coordination, Renee DiResta et al. asserts, "robust collaboration between government agencies, platforms, and private companies is key to combating this threat [influence operations]."[28] Although a consensus exists for a multi-stakeholder approach, Christina Nemr and William Gangware point out that it is not quite clear which entity, the U.S. government or the private sector, is or should be organizing and leading such coordination.[29] In fact, Alina Polyakova argues, "The greatest challenge facing the U.S. government as it has sought to craft a counter disinformation strategy has been identifying the appropriate coordinating body able to carry out a politically empowered policy agenda."[30] An examination of the literature about the roles of prominent key stakeholders, such as U.S. government agencies and private sector media companies, and the complexities of the threat will serve as a starting point to understand these challenges and provide some clarity to help facilitate the development and implementation of a response strategy.

1. The Complex, Ambiguous, and Evolving Threat Picture

Throughout the literature, it is evident that defining and describing the deceptive messaging threat and its components in a simplified and comprehensible way is no easy feat. Claire Wardle and Hossein Derakhshan support Fly, Rosenberger, and Salvo and state,

---

[28] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 101.

[29] Nemr and Gangware, *Weapons of Mass Distraction*, 37.

[30] *United States Senate Foreign Relations Subcommittee on State Department and USAID Management, International Operations, and Bilateral International Development Hearing on "The Global Engagement Center: Leading the United States Government's Fight against Global Disinformation Threat,"* Senate, 116th Cong., 2nd sess., March 5, 2020, 6, https://www.foreign.senate.gov/imo/media/doc/030520_Polyakova_Testimony.pdf.

"the absence of definitional rigour" and the resulting "failure to recognize the diversity of mis- and dis-information" is a fundamental reason for slow progress in addressing the threat.[31] After conducting a literature review, Joshua Tucker et al. echoed the same sentiment that a lack of consensus exists for defining "disinformation, misinformation, online propaganda, hyperpartisian news, fake news, clickbait, rumors, and conspiracy theories."[32] This challenge has resulted in a spectrum of interpretations of what the deceptive messaging threat constitutes.

Experts' interpretations of what comprises the deceptive messaging threat range from narrow and simple definitions to very broad and comprehensive. Soroush Vosoughi, Deb Roy, and Sinan Aral framed the problem in one study by only differentiating between authentic and false information.[33] Whereas Nemr and Gangware have a more moderate frame of reference and define the problem as, "the purposeful dissemination of false information intended to mislead or harm," while also recognizing that disinformation "can consist of true facts, pieced together to portray a distorted view of reality."[34] Expanding on more moderate definitions, Jennifer Kavanagh and Michael Rich describe the threat to democracy as a more extensive, and far less black or white, problem of "truth decay."[35] They define the four trends of truth decay as "increasing disagreement about facts and analytical interpretations of facts and data, a blurring of the line between opinion and fact, increasing relative volume, and resulting influence, of opinion and personal experience

---

[31] Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Report Number DGI(2017)09 (Strasbourg, France: Council of Europe, 2017), 15, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

[32] Joshua A. Tucker et al., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature* (Menlo Park, CA: Hewlett Foundation, 2018), 55, https://hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf.

[33] Vosoughi, Roy, and Aral, "The Spread of True and False News Online," 1146.

[34] Nemr and Gangware, *Weapons of Mass Distraction*, 4.

[35] Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, RR-2314-RC (Santa Monica, CA: RAND, 2018), 11, https://www.rand.org/pubs/research_reports/RR2314.html.

over fact, and declining trust in formerly respected sources of factual information."[36] Each definition is not necessarily incorrect; however, if each of these were applied to collect data in the information space, a significant contrast would likely appear, and perhaps disagreement, in the resulting data sets.

Although scholarly definitions of the deceptive messaging threat vary in specifics, at a foundational level, they have more similarity and consensus. Nemr and Gangware point out three fundamental converging factors common throughout all the literature defining the deceptive messaging threat, "technology, media, and human behaviors."[37] Other authors have also attempted to simplify the complexities of the deceptive messaging threat with new terminology or frameworks that still effectively capture the nuances that may vary.

Sam Korta uses the phrase "counterfeit narrative" throughout her research and argues, "more so than terms like "fake news" or "conspiracy theories," counterfeit narrative more effectively captures the nuances of the disinformation, the actors disseminating it, and the spreadability of that propaganda online."[38] Korta, in parallel with Kirill Meleshevich and Bret Schafer, also proposed an information-laundering model based on money laundering concepts.[39] These authors used the laundering models to illustrate how inauthentic content travels through the internet ecosystem to appear legitimate.[40] Korta contends that her model "helps frame the issue in a way that homeland security professionals, law enforcement, policymakers, and the general public can understand."[41] Similarly, Bodine-Baron et al. developed a framework called the Russian disinformation

---

[36] Kavanagh and Rich, *Truth Decay*, x–xi.

[37] Nemr and Gangware, *Weapons of Mass Distraction*, 3.

[38] Korta, "Fake News, Conspiracy Theories, and Lies," xvi.

[39] Korta, 79–97; Kirill Meleshevich and Bret Schafer, *Online Information Laundering: The Role of Social Media* (Washington, DC: Alliance for Securing Democracy, 2018), 4, https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/.

[40] Korta, 79–97; Meleshevich and Schafer, 4.

[41] Korta, xvii.

chain to demonstrate each step in the disinformation campaign process visually.[42] The authors assert that "by simplifying the framework to basic components we can illustrate where current proposed policies to address Russian influence are concentrated, and where gaps might exist."[43] Although these frameworks appear to be a step in the right direction, not all scholars agree on the effectiveness of models and frameworks used to describe the information environment.

The information environment is a rapidly evolving element of the deceptive messaging threat, and Rand Waltzman takes a more skeptical stance and states that the information environment is evolving too fast for current models to remain relevant.[44] Although unconvinced about current models, Waltzman supports the development of a "Center for Cognitive Security" that can create and maintain information environment models.[45] Despite widespread inconsistencies about framing, defining, and illustrating the deceptive messaging threat, scholars are more unified concerning other elements of the deceptive messaging threat.

Many authors, in support of Waltzman, find that the architecture of the information environment and the evolution of technology present significant challenges to combating deceptive messaging. One challenge is the attribution of deceptive message sources and the ability for nefarious actors to operate with anonymity. Suzanne Spaulding, Devi Nair, and Arthur Nelson explain, "there exist few technical processes or solutions that can, with full certainty, determine the originating sources of online activity."[46] The difficulty of attribution, as Sophi Ignatidou points out, directly conflicts with guidelines for the U.S.

---

[42] Bodine-Baron et al., *Countering Russian Social Media Influence*, x.

[43] Bodine-Baron et al., 7–8.

[44] Rand Waltzman, *The Weaponization of Information: The Need for Cognitive Security*, CT-473 (Santa Monica, CA: RAND, 2017), 2, http://www.rand.org/pubs/testimonies/CT473.html.

[45] Waltzman, 7.

[46] Suzanne Spaulding, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System* (Washington, DC: Center for Strategic International Studies, 2019), 10, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf.

Department of Justice (USDOJ) to disclose information about foreign influence.[47] These guidelines require a high-confidence attribution to a foreign government, which thus restricts its ability to act on the many unattributable campaigns or those of domestic origins.[48] With the conflict between enforcement and attribution, Bradley Hanlon suggests that online platforms have more flexibility in terms of response since attribution is not necessary for them to take action against inauthentic behavior.[49] Ignatidou takes a similar stance for the government and recommends that "EU and U.S. policymakers should not get fixated on specific agents as such an approach would be counterproductive."[50] In addition to identifying the actors behind deceptive messaging campaigns, the authors are also concerned about the visibility of future deceptive messaging campaigns.

Building on the challenges of attribution, Renee Diresta, the Director of Research at New Knowledge, predicts that deceptive behavior online will become more difficult to identify with greater "misuse of less popular and less resourced social platforms, and an increase in the use of peer-to-peer messaging services," to avoid detection from law enforcement.[51] Such developments can possibly render the tracking or debunking of deceptive activity more difficult than it already is. On a similar note, Nemr and Gangware anticipate that encryption technology and artificial intelligence will also further complicate attribution or identification of deceptive messaging moving forward.[52] In addition to new technology hampering attribution, Ignatidou points out, "'datafication' of different aspects

---

[47] Sophia Ignatidou, *EU–U.S. Cooperation on Tackling Disinformation* (London: Chatham House, 2019), 19–20, https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf.

[48] Ignatidou, 19–20.

[49] Bradley Hanlon, *A Long Way to Go: Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*, no. 041 (Washington, DC: German Marshall Fund, 2018), 12, https://securingdemocracy.gmfus.org/wp-content/uploads/2018/12/A-Long-Way-to-Go-Analyzing-Facebook-Twitter-and-Googles-Efforts-to-Combat-Foreign-Interference.pdf.

[50] Ignatidou, *EU–U.S. Cooperation on Tackling Disinformation*, 34.

[51] *Foreign Influence Operations and their Use of Social Media Platforms: Hearing before the Select Committee on Intelligence*, Senate, 115th Cong., 2nd sess., August 1, 2018, 5, https://www.intelligence.senate.gov/sites/default/files/documents/os-rdiresta-080118.pdf.

[52] Nemr and Gangware, *Weapons of Mass Distraction*, 42.

of life, the rise of smart homes and smart cities, the Internet of Things (IoT), accelerating artificial intelligence (AI) development, and internet and mobile phone penetration, have vastly exacerbated the combined ripple effects of disinformation's complexity and scale."[53] The recognition of the challenges about the architecture of the information environment and rapidly evolving technology by leading scholarship are also well balanced with consideration for the preservation of democratic values.

The concern among scholars for the protection of the First Amendment and privacy rights is high. Ashley Deeks, Sabrina McCubbin, and Cody Poplin point out that free speech has always relied on credible and natural regulators, such as experienced editors or producers, and those no longer exist with the advent of social media.[54] Without those regulators in place, Fly, Rosenberger, and Salvo emphasize that response efforts must not inadvertently undermine democracy by violating such protections.[55] The difficulty these authors have had to define and frame the problem combined with the need for practitioners to adapt to evolving technology while also balancing democratic values all contribute to the complexity and ambiguity of the deceptive messaging threat.

2. Accountability and Leadership

A general consensus is present in the literature that an effective response to combat deceptive messaging is going to require wide-ranging participation and cooperation from a blend of U.S. government agencies, private sector companies, researchers and academia, civil society, and the public.[56] However, Clint Watts argues that the United States lacks

---

[53] Ignatidou, *EU–U.S. Cooperation on Tackling Disinformation*, 5.

[54] Ashley Deeks, Sabrina McCubbin, and Cody M. Poplin, "Addressing Russian Influence: What Can We Learn from U.S. Cold War Counter-Propaganda Efforts?" *Lawfare*, October 25, 2017, https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts.

[55] Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 19.

[56] Claesson, "Coming Together to Fight Fake News," 13–19; Hanlon, *A Long Way to Go*, 10–12; Waltzman, *The Weaponization of Information*, 4; Bodine-Baron et al., *Countering Russian Social Media Influence*, xiii; Mark Warner, "A New Doctrine for Cyberwarfare & Information Operations" (speech, Center for a New American Security, December 7, 2019), https://www.warner.senate.gov/public/index.cfm/2018/12/warner-calls-for-society.

the leadership needed to defend the country from foreign influence.[57] A divergence and lack of clarity exists in the literature when it comes to pinpointing which of those entities should lead and coordinate response efforts. James Farewell supports Watts' argument by pointing out the ineffectiveness of the GEC, the U.S. government agency tasked with leading the federal government response to propaganda and disinformation.[58] Farwell further asserts that the GEC will not be effective alone due to a lack of strategy and resources.[59] Other scholars have responded to such claims about leadership by suggesting which entity would be best suited for overseeing and coordinating deceptive messaging response efforts.

Nemr and Gangware point out the way in which deceptive messages are spread on internet platforms combined with their seemingly geopolitical objectives creates a conflict of accountability between the government and the private sector.[60] Despite this conflict, Nemr and Gangware's position is "social media and technology companies are well-placed to lead these efforts, in collaboration with governments and other partners."[61] However, others, such as Sijbren De Jong et al., argue that governments must be proactive to protect their citizens from the threat of deceptive messaging because "the principal task of liberal democratic governments is to protect the safety, security and wellbeing of its citizens, at the same time as it is to uphold and protect the democratic constitutional order."[62] This conflict is evident, as two dominant schools of thought are apparent in the literature, one

---

[57] Clint Watts, *Messing with the Enemy* (New York: Harper, 2018), loc. 3203 of 4555, Kindle.

[58] James P. Farwell, "Countering Russian Meddling in U.S. Political Processes," *Parameters* 48, no. 1 (Spring 2018): 40, https://www.socom.mil/SovereignChallenge/Sovereign%20Challenge%20Publications/Countering%20Russian%20Meddling%20in%20US%20Political%20Processes.pdf; John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law 115-232, *U.S. Statutes at Large* 132 (2018): 2076–2078, https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

[59] Farwell, "Countering Russian Meddling in U.S. Political Processes," 40.

[60] Nemr and Gangware, *Weapons of Mass Distraction*, 37–38.

[61] Nemr and Gangware, 37–38.

[62] Sijbren De Jong et al., *Inside the Kremlin House of Mirrors: How Liberal Democracies Can Counter Russian Disinformation and Societal Interference* (The Hague, Netherlands: The Hague Centre for Strategic Studies, 2017), 2, https://hcss.nl/report/inside-kremlin-house-mirrors-how-liberal-democracies-can-counter-russian-disinformation-0.

in support for a private sector led approach with greater self-regulation, and the other advocating for a government agency led approach with more oversight and regulation.

The push for self-regulation of private sector companies, primarily social media platforms, was palpable after the 2016 U.S. presidential elections. Gabriel Kahn, the Director of the Future of Journalism at the University of Southern California, was quoted in a December 2016 article, "Facebook and other platforms bear enormous responsibility here. A supermarket doesn't stock fake milk on its shelves, so the largest distributor of news shouldn't be complicit in pushing erroneous information with no filter."[63] Along the same lines, Jonathon Morgan, the CEO of New Knowledge and previous White House and State Department advisor, wrote an opinion piece in October 2017 titled "Facebook and Google need to own their role in spreading misinformation—and fix it."[64] He went on to argue, "every tech worker and executive has an ethical responsibility to protect our democratic ideals."[65] Mentions of the U.S. government in these pieces were largely non-existent.

Over time, authors began recognizing the inadequacy of self-regulation efforts. Bradley Hanlon, who supports self-regulation, began to publicly admit that social media company self-regulation efforts were insufficient due to a lack of coordination between companies, presence of inauthentic accounts, and inability for companies to "clearly state and consistently enforce their terms of service."[66] More recent publications still echo Hanlon's unsatisfactory conclusions. The European External Action Service (EEAS) recognized that the efforts from social media companies have improved, however, even after the latest measures taken to combat disinformation during the Coronavirus pandemic

---

[63] Ian Chaffee, "Who's to Blame for Fake News and What Can Be Done about It?," USC News, December 15, 2016, https://news.usc.edu/113738/whos-to-blame-for-fake-news-and-what-can-be-done-about-it/.

[64] Jonathon Morgan, "Facebook and Google Need to Own their Role in Spreading Misinformation—and Fix It," October 9, 2017, https://www.cnn.com/2017/10/09/opinions/social-media-platforms-spreading-disinformation-opinion-morgan/index.html.

[65] Morgan.

[66] Hanlon, *A Long Way to Go*, 3–7.

it claimed, "platforms have difficulties adhering to their own published standards and public commitments on preventing the proliferation of dangerous coronavirus-related disinformation, despite allocating significant resources to this task."[67] The inadequacies of private sector companies' ability to effectively self-regulate are a prominent dispute in the discourse to a private sector-led approach.

In addition to the less than favorable self-regulation efforts, Laura Rosenberger testified at a Senate Select Committee on Intelligence hearing in 2018 and explained that large social media companies are just one piece of the information ecosystem and that the scope of the problem extends beyond giants like Twitter and Google.[68] Echoing Rosenberger's point, Bodine-Baron et al. explains that adversaries will "adapt to countermeasures, create or co-opt new willing proxies, or migrate to more-permissive platforms."[69] Further complicating the problem, multi-disciplinary experts from the United States, Canada, and Europe argue that disinformation is not just a technical problem, but "also a social and economic problem."[70] The less than favorable results from self-regulation efforts, as well as unavoidable challenges of the information space produced discussions of a government-driven alternative.

The government-led approach proposed by some authors would simply reinforce policies, laws, and coordination efforts, not replace them. Dipayan Ghosh and Ben Scott argue, "We cannot expect them [digital media platforms and companies] to regulate themselves. As a democratic society, we must intervene to steer the power and promise of

---

[67] "EEAS Special Report: Disinformation on the Coronavirus—Short Assessment of the Information Environment," EEAS Strategic Communications and Information Analysis Division, March 19, 2020, https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/.

[68] *Statement of Laura Rosenberger Alliance for Securing Democracy, the German Marshall Fund of the United States before the United States Senate Select Committee on Intelligence Concerning "Foreign Influence Operations and their Use of Social Media Platforms,"* Senate, 115th Cong., 2nd sess., August 1, 2018, 2, https://securingdemocracy.gmfus.org/wp-content/uploads/2018/07/ROSENBERGER_SSCI-statement_Foreign-Influence-Ops-on-Social-Media_08-01-1....pdf.

[69] Bodine-Baron et al., *Countering Russian Social Media Influence*, 31.

[70] Canadian Security Intelligence Service, *Who Said What?*, 104.

technology to benefit the many rather than the few."[71] In parallel, Alina Polyakova and Daniel Fried agree that social media companies should not "be the 'arbiters of truth'" and suggest that the U.S. government, in conjunction with other nations, should reinforce and advocate for social media companies' participation in building long-term resilience.[72] The consensus for a government-led approach has grown in popularity in dominant literature.

Despite some existing consensus for a government-led approach, the degree in which the U.S. government should be involved in response efforts is still debated. Although an advocate for targeted government regulation, Paul Barrett pushes for social media companies to do more proactive self-regulation to prevent government overreach.[73] To support his argument, Barrett points out that too much government involvement could result in censorship and a violation of the First Amendment; however, companies moderating content on their platforms that violate policies is well within the law.[74] Cass Sunstein presents a similar argument noting that the regulation of communication channels is inevitable; it is just a matter of what kind of regulation.[75] Sunstein supports his argument by explaining how the media has been regulated over the past several decades with the issuance of licenses and creation of laws to protect property rights.[76] Although more ambiguous, the desire and inevitability for government regulation that drives response efforts forward is apparent.

---

[71] Dipayan Ghosh and Ben Scott, *#DigitalDeceit: The Technologies behind Precision Propaganda on the Internet* (Washington, DC: New America, 2018), 4, https://d1y8sb8igg2f8e.cloudfront.net/documents/digital-deceit-final-v3.pdf.

[72] Daniel Fried and Alina Polyakova, *Democratic Defense against Disinformation* (Washington, DC: Atlantic Council, 2018), 10–14, https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf.

[73] Paul Barrett, *Tackling Domestic Disinformation: What the Social Media Companies Need to Do* (New York City: NYU Stern, 2019), 22, https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_domestic_disinformation_digital?e=31640827/68184927.

[74] Barrett, 20.

[75] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton, NJ: Princeton University Press, 2017), 178–182.

[76] Sunstein, 178–182.

In alignment with these conversations of government-driven response efforts to deceptive messaging, the Countering Foreign Influence Subcommittee tasked DHS in 2019 to become the leading entity to establish a national strategy to counter foreign influence and ensure effective coordination among the government, as well as social media companies.[77] While commentary or analyses about these efforts has yet to be seen, the growing support among scholars for the government to take a leadership role and the documented tasking of DHS are a promising step toward resolving the gap in leadership and the development of a coordinated national strategy across all stakeholders.

[77] Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*, 10.

II. THE U.S. RESPONSE STRATEGY PLAYBOOK

This chapter expands on two categories of strategic recommendations common in the literature, public resilience and coordination. It outlines the main concepts within each category and compares them to the deceptive messaging response efforts in the United States. Chapter III follows with a case study of the EU's response to disinformation and presents key takeaways and lessons for potential application in the United States. The EU case study contains valuable insights, but it does not provide explicit steps or methods to achieve a more unified approach. Therefore, Chapter IV introduces collective impact as a cross-sector coordination method and assesses it for suitability to address the deceptive messaging threat. Based on the findings from the case study and assessment, Chapter V concludes with recommendations to facilitate the development of a unified approach to combat the threat.

Strategists have proposed an array of mitigation measures for the U.S. government to deploy to promote a society more resilient to the deceptive messaging campaigns that threaten the nation's democracy. The broad spectrum of recommendations addresses improvements to many different elements of society from AI research to automate the detection of deception to U.S. government policy that governs transparency. While the sheer number of recommendations that have been put forth are seemingly overwhelming, they each play a critical role in a more comprehensive approach to addressing the deceptive messaging threat. In her earlier testimony before Congress, Alina Polyakova, an expert on the subject from the Brookings Institution, expressed that there is no "silver bullet" for the problem.[78] With no one approach being the correct or only solution, the prioritization of such recommendations will be necessary as the U.S. government begins to mount a response.

---

[78] *United States House Committee on Appropriations—Subcommittee on State, Foreign Operations, and Related Programs United States Efforts to Counter Russian Disinformation and Malign Influence,* House of Representatives, 116th Cong., 1st sess., July 10, 2019, 2, https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-PolyakovaA-20190710.pdf.

To initiate the prioritization process, I categorized the sample of strategy proposals made by think tanks, academics and scholars, a security advocacy group, research institutes, private sector consulting companies, and government practitioners into themes. The strategy proposals analyzed were largely categorized into five major themes: (1) public resilience, (2) policy and regulation, (3) coordination, (4) research and development, and (5) operational activities. The identification of these themes can help streamline the creation of a framework for a comprehensive strategy for the U.S. government and simplify decision-makers' understanding of their options.

Out of the five themes identified, a majority of the recommendations primarily fell under two categories, (1) public resilience, and (2) coordination. An in-depth review of all five categories would have been much too large for this thesis. Therefore, this chapter highlights the significant recommendations and subcategories within those two themes and offers observations about U.S. government efforts in each domain.

A. PUBLIC RESILIENCE

Deceptive messaging campaigns seek to influence American audiences by exploiting human cognition and decision making through the manipulation and distortion of information.[79] In other words, every individual in the world represents a potential point of vulnerability and the public's resilience, or cognitive security, is a critical component to be addressed. Some experts believe that by fostering an informed and educated public, through a variety of means, society will be more resilient and less susceptible to malign influence operations.[80] In fact, Spaulding, Nair, and Nelson argue that an "informed and engaged public" is the best defense against disinformation.[81] The dominant literature

---

[79] Mustafa Canan and Rik Warren, "Cognitive Schemas and Disinformation Effects on Decision Making in Lay Populations" (paper presented at the 13th International Conference on Cyber Warfare and Security (ICCWS 2018), Washington, DC, March 24, 2018), 1, https://www.researchgate.net/publication/327845605_Cognitive_Schemas_and_Disinformation_Effects_on_Decision_Making_in_Lay_Populations.

[80] Barrett, *Tackling Domestic Disinformation*, 23–26; Hanlon, *A Long Way to Go*, 3–7; Korta, "Fake News, Conspiracy Theories, and Lies," 117–119.

[81] Spaulding, Nair, and Nelson, *Beyond the Ballot*, 34.

identified three leading approaches to building public resilience: government transparency, awareness campaigns, and media literacy initiatives.

Although these approaches were popular among the collective, they do not represent all the potential ways in which the United States can better engage the public. Each approach can contribute to public resilience in different ways. For the purposes of this research, these subcategories are defined as the following.

- **Government transparency:** The unsolicited disclosure of information about the deceptive messaging threat and the U.S. government response to the public.
- **Awareness campaigns:** The medium in which publicly available information about deceptive messaging is disseminated and presented to stakeholders and/or society.
- **Media literacy initiatives:** efforts to provide people of all demographics with the skills, as Alice Huguet et al. define, "to access, analyze, evaluate, and communicate messages in a wide variety of forms."[82]

Collectively, the three subcategories intend to create an environment in which individuals can make independent, informed, and educated decisions that are less susceptible to deceptive messages.

1. Government Transparency

Specific to the deceptive messaging threat, the U.S. government's transparency practices are inadequate, especially when compared to international efforts. This research discovered just a few official reports from U.S. government institutions about the threat and response efforts, which have received minimal attention or were challenging to find. The information available is largely produced by think tanks and academics, not the U.S. government. It is worth noting that the U.S. government funded and sponsored some of the

[82] Alice Huguet et al., *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay*, RR-3050-RC (Santa Monica, CA: RAND, 2019), x, https://www.rand.org/pubs/research_reports/RR3050.html.

reports published by think tanks and academics; however, the products typically do not reflect the views of the government.[83] In contrast, EU institutions have regularly released dozens of press releases, reports, and updates to the public about the disinformation threat and their response since it began in 2015 (discussed further in Chapter III).[84] The threat to national security and vulnerability of the population demands more adequate efforts to keep the public informed.

Despite these shortcomings, it would be shortsighted not to point out some of the recent efforts of the U.S. government that reflect better transparency practices. One illustration is the decision of the USDOJ to release the *Report on the Investigation into Russian Interference in the 2016 Presidential Election* in March 2019.[85] Although heavily redacted, the report provides information that describes how Russia used deceptive tactics on social media to "sow discord in the U.S. political system."[86] Another example is the introduction of the Deepfake Reports Act (DRA) in July 2019. The DRA "directs the Department of Homeland Security (DHS) to produce periodic reports on deepfakes to raise public awareness of possible fraudulent or misleading content, improve our understanding of the technology used to generate deepfakes, and identify how foreign governments or their proxies use the technology to harm national security."[87] These actions are a positive progression towards greater transparency.

To improve the U.S. government transparency, experts proposed a variety of recommendations via communication and legislative measures. De Jong et al. presented a

---

[83] Nemr and Gangware, *Weapons of Mass Distraction*, acknowledgements; Nicole Peterson, ed., *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper* (Washington, DC: Department of Defense, Strategic Multilayer Assessment Program, 2019), acknowledgements, https://www.politico.com/f/?id=0000016b-a5a1-d241-adff-fdf908e00001.

[84] European Commission, "Tackling Online Disinformation."

[85] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 1–185.

[86] Mueller, 4.

[87] "Peters, Portman Bill Responding to Growing Threat of Deepfakes Advances in Senate," U.S. Senate Committee on Homeland Security and Governmental Affairs, July 26, 2019, https://www.hsgac.senate.gov/media/minority-media/peters-portman-bill-responding-to-growing-threat-of-deepfakes-advances-in-senate.

more straightforward recommendation that "Governments should acknowledge what societal issues Russian information operations may (seek to) exploit and communicate with the general population the steps they intend to take, without becoming alarmist."[88] Other suggestions called for the introduction, passing, and enforcement of legislation that drives better transparency, which can often be a difficult and time-consuming process. Fly, Rosenberger, and Salvo argued, "Congress should help foster a culture of transparency...by passing legislation that ensures Americans know the sources of online political ads."[89] Similarly, Robert Blackwill and Philip Gordon called for legislation to "enhance transparency requirements" in the context of campaign finance laws.[90] Political ads and campaign finance related transparency would not be broad enough to expose the public to the dangers of deceptive messaging. Therefore, legislation to drive transparency of other stakeholders was also popularly suggested.

Although this research is mostly concerned with the response of the U.S. government, the bulk of the other transparency recommendations revolved around social media platforms and private sector companies. To establish standards and accountability for private sector companies, Blackwill and Gordon recommend that the U.S. government should create a voluntary code of conduct, similar to the code that the EU implemented in 2018.[91] They continue to say that the standards should include monitoring their platforms for "disinformation, false news stories, botnets, and false-flag advertising—identifying, labeling, and blocking them where appropriate."[92] Legislation that targets social media

---

[88] De Jong et al., *Inside the Kremlin House of Mirrors*, 3.

[89] Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 6.

[90] Robert D. Blackwill and Philip H. Gordon, *Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge* (Washington, DC: Council on Foreign Relations, 2018), 21, https://www.cfr.org/report/containing-russia.

[91] Blackwill and Gordon, *Containing Russia*, 32; European Commission, "Code of Practice on Disinformation," Digital Single Market, September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[92] Blackwill and Gordon, 32.

companies must be carefully considered as not all platforms are created equal and the encroachment on free speech and the open internet may be counterintuitive.

These examples are just a few of the prescriptions experts made regarding U.S. government transparency practices. Better transparency efforts, however, is useless if it is not disseminated in a way for the public to find or understand easily. To build upon transparency efforts, other authors focused on recommendations that intend to raise the level of awareness of American society with publicly available information.

2. Awareness Campaigns

Awareness campaigns build on the concept of greater transparency, and can be used by U.S. government and non-governmental entities to help educate the public about the threat and response. Fly, Rosenberger, and Salvo proposed that the government entity that tracks influence operations should share the information with the public when possible.[93] Such campaigns could be strategic or tactical in nature. Timely awareness campaigns can help the public evaluate information they are consuming in real-time, whereas strategic campaigns will help both practitioners and the public understand the broader, long-term implications of deceptive messaging campaigns. Some authors, such as Martin Innes et al., find that real-time tactical awareness campaigns are critical to diminish the opportunity for rumors to develop.[94] While both types of campaigns have value, an opportunity exists to make an impact now with real-time tracking projects that have been developed by civil society.

The most notable examples of current awareness campaigns were created by non-governmental entities, such as the Alliance for Securing Democracy's (ASD) Hamilton 68

---

[93] Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 25.

[94] Martin Innes et al., *From Minutes to Months: A Rapid Assessment of the Impact of Media and Social Media during and after Terror Events* (Cardiff, UK: Cardiff University, Crime & Security Research Institute, 2018), 61, https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bc74f950d929708f7733b3c/1539788716177/M2M+Report+%5BFinal%5D.pdf.

dashboard.[95] Hamilton 68 was designed to "expose the effects of Russian online influence networks in real-time and to inform the public of themes and content being promoted to Americans by foreign powers."[96] In 2019, the ASD launched the second version of Hamilton 68 that expanded on the features and data from the first version.[97] The public exposure of such activity provides just one resource for the public or even practitioners to use while evaluating information they consume.

Some U.S. government agencies have begun to produce other awareness campaigns. One example is the Cybersecurity and Infrastructure Protection Agency's (CISA) one-page public document, titled *The War on Pineapple* (Appendix A), that illustrates how foreign interference operations are carried out in simple terms that can be understood by the average person.[98] The DHS website recently posted a number of similar one-page products about foreign influence, as well as how to recognize, question, and investigate deceptive messages.[99] These efforts are at a nascent stage and authors are seeking to expand them in their recommendations.

To accomplish the expansion of awareness campaigns, experts highlight the benefits of the government supporting non-governmental efforts rather than duplicating them. Fried and Polyakova claim civil society groups are more capable than the government to identify deceptive activity in real-time, citing "Ukraine's StopFake, Bellingcat, the Atlantic Council's Digital Forensic Research Lab, the Alliance for Security

---

[95] Laura Rosenberger and J. M. Berger, "Hamilton 68: A New Tool to Track Russian Disinformation on Twitter," Alliance for Securing Democracy, August 2, 2017, https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/.

[96] Deeks, McCubbin, and Poplin, "Addressing Russian Influence."

[97] "Hamilton 2.0 Dashboard," Alliance for Securing Democracy, accessed September 7, 2019, https://securingdemocracy.gmfus.org/hamilton-dashboard/.

[98] Cybersecurity and Infrastructure Security Agency, *The War on Pineapple: Understanding Foreign Interference in 5 Steps* (Rosslyn, Arlington, VA: Cybersecurity and Infrastructure Security Agency, 2019), 1, https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf.

[99] "Foreign Interference," Department of Homeland Security Cybersecurity and Infrastructure Security Agency, last revised December 2, 2019, https://www.cisa.gov/publication/foreign-interference.

Democracy's Hamilton 68, EU DisinfoLab, and the Baltic Elves" as proven examples.[100] In support of their argument, Deeks, McCubbin and Poplin point out that funding and support of non-governmental efforts is a more sustainable path forward since the threat of deceptive messaging will be persistent.[101] Support of existing awareness campaigns can be a force multiplier for the U.S. government to bolster its response efforts.

Despite the benefits of the U.S. government funding non-governmental efforts, such a relationship can come with some potential risk. Polyakova and Fried push for the government and private sector to fund civil society efforts; however, they highlight that funding sources can create undue bias and undermine the public's perceived integrity of the initiative.[102] This concern is supported by dissent within the EU. The Dutch parliament has requested the European Commission to shut down EU vs Disinfo, a government funded project to track disinformation campaigns, with concern that it does not have the right to determine what is true or false.[103] With the appropriate safeguards to prevent bias, civil society provides a tremendous opportunity for the United States to leverage in protecting its society through awareness campaigns.

3. Media Literacy

The internet has become a primary source of information and news for American society. Several authors highlighted that educational efforts for consuming and sharing

---

[100] Alina Polyakova and Daniel Fried, *Democratic Defense against Disinformation 2.0* (Washington, DC: Atlantic Council Eurasia Center, 2019), 3, https://www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation-2-0.

[101] Deeks, McCubbin, and Poplin, "Addressing Russian Influence."

[102] Polyakova and Fried, *Democratic Defense against Disinformation 2.0*, 3.

[103] European Commission, "C(2019) 58 Final" (official memorandum, Brussels: European Commission, 2019), 3–9, https://ec.europa.eu/dgs/secretariat_general/relations/relations_other/npo/docs/netherlands/2018/com20180236/com20180236_eerstekamer_reply_en.pdf.

information in the current environment are necessary but deficient.[104] Timothy McGeehan argued, "Western nations need to reinvigorate their civics and social studies programs as well as focus on 'digital literacy' to build citizens into "hard targets" for disinformation."[105] Singer and Brooking concurs and go as far to say, "information literacy is no longer merely an education issue but a national security imperative."[106] Huguet et al. supports McGeehan, Singer, and Brooking, and find that to be more effective, individuals need "the ability to evaluate sources, synthesize multiple accounts into coherent understanding of an issue, understand the context of communications, and responsibly create and share information."[107] Media literacy recommendations from experts go hand in hand with the themes identified in public resilience, which focus on education and skill development to consume information responsibly and become less susceptible to deceptive messaging.

Despite the apparent importance of education and literacy to combat deceptive messaging, it is equally apparent that U.S. society lacks the skills needed to navigate the 21st century information environment. Huguet et al. further remarks that it is not clear neither K-12 students nor adults are competent in such skills.[108] To support their claim, Stanford researchers found that American students in middle school through college show "a dismaying inability...to reason about information they see on the Internet."[109] The

---

[104] Timothy McGeehan, "Countering Russian Disinformation," *Parameters* 48, no. 1 (Spring 2018): 54–56, https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf; Huguet et al., *Exploring Media Literacy Education*, 1; Brooke Donald, "Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online," Stanford Graduate School of Education, November 22, 2016, https://ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility-information-online.

[105] McGeehan, 56.

[106] P. W. Singer and Emerson Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018), loc. 4535 of 10056, Kindle.

[107] Huguet et al., *Exploring Media Literacy Education*, ix.

[108] Huguet et al., 1.

[109] Donald, "Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online."

authors point to outdated curricula as a potential contributing factor to their findings.[110] Deceptive messages will continue to be effective if society does not have the education nor skills to differentiate between fact, falsehood, or opinion.

Similarly to awareness campaigns, some of the educational gap has been filled in by non-governmental agencies, some of which partner with the government. One initiative considered a success is the Facebook Global Digital Challenge, which is sponsored by the U.S. Department of Defense (DOD) and U.S. Department of State (DOS).[111] The program was designed for students across the world to design and implement a social or digital initiative to combat hate and extremism, some of which included disinformation.[112] Although the initiatives' website boasts to have served over 1,000 academic institutions, only a small fraction appear to fall within the United States.[113] Despite these efforts, based on researchers findings, it is evident such skills need to be taught on a far more extensive scale.

Some experts believe the U.S. government should be doing more to bolster educational efforts more broadly. De Jong et al. argue, "governments bear a special responsibility to instill media literacy courses in the secondary and tertiary school curriculum."[114] Other experts also pointed out that these education efforts should also incorporate government officials and journalists.[115] To support De Jong et al.'s argument, some scholars point to Finland's educational efforts and resiliency to Russian disinformation as an example to model after the Open Society Institute in 2018 gave

---

[110] Donald.

[111] "Our Work," EdVenture Partners, accessed September 2, 2019, https://www.edventurepartners.com/our-work.

[112] EdVenture Partners.

[113] "About," EdVenture Partners, accessed July 17, 2020, https://www.edventurepartners.com/about.

[114] De Jong et al., *Inside the Kremlin House of Mirrors*, 4.

[115] Blackwill and Gordon, *Containing Russia*, 54; Innes et al., *From Minutes to Months*; De Jong et al., *Inside the Kremlin House of Mirrors*.

Finland the highest media literacy score out of 35 European countries.[116] The study correlates Finland's, and other Northwestern European nations', resilience to deceptive messaging largely to their public educational systems and emphasis on media literacy, but mentions more research to confirm a relationship is needed.[117] Marin Lessenski, Programme Director for European Policies at OSI-Sofia, states, "Finland's government considers the strong public education system as a main tool to resist information warfare against the country."[118] Broader educational reforms, as seen in Finland, would be one way to scale media literacy efforts in the United States.

To support the findings of the OSI-Sofia report, other research and anecdotes provide strong indications that media literacy has positive effects to help individuals detect deceptive messaging. Huguet et al. found that "Past research has identified some evidence that ML [media literacy] increases participant resiliency to disinformation and is able to change the way participants consume, create, and share information. However, there is little causal, evaluative research in the ML field that isolates the effects of ML interventions."[119] Anecdotal evidence is also available to help support these findings. Cambridge University's online game that "works like a 'vaccine', increasing skepticism of fake news by giving people a 'weak dose' of the methods behind disinformation," is a notable example.[120] Early evidence from the game suggests it has been successful. One study claims, "the perceived reliability of fake news before playing the game had reduced

---

[116] Marin Lessenski, *Common Sense Wanted Resilience to 'Post-Truth' and its Predictors in the New Media Literacy Index 2018* (Sofia, BG: Open Society Institute–Sofia, 2018), 3–13, https://osis.bg/wp-content/uploads/2018/04/MediaLiteracyIndex2018_publishENG.pdf.

[117] Lessenski, 11.

[118] Emma Charlton, "How Finland is Fighting Fake News—in the Classroom," World Economic Forum, May 21, 2019, https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/.

[119] Huguet et al., *Exploring Media Literacy Education*, website summary.

[120] Fred Lewsey, "Fake News 'Vaccine' Works: 'Pre-Bunk' Game Reduces Susceptibility to Disinformation," University of Cambridge, June 25, 2019, https://www.cam.ac.uk/research/news/fake-news-vaccine-works-pre-bunk-game-reduces-susceptibility-to-disinformation.

by an average of 21% after completing it."[121] The limited, yet positive, evidence available for media literacy initiatives offers some indication that broader educational efforts may be valuable in building individual resilience to deceptive messaging.

Some steps have been taken to scale media literacy efforts in U.S. society. In July 2019, Senator Amy Klobuchar introduced the Digital Citizenship and Media Literacy Act that "would create a grant program at the Department of Education to help develop digital and media literacy education across grades K-12."[122] Such educational initiatives are a positive step toward the recommendations that experts have made to provide American citizens with the skills necessary to consume and evaluate information effectively.

B. COORDINATION

Different stakeholders within the U.S. government, the private sector, and civil society have ramped up efforts since the 2016 U.S. presidential elections to combat deceptive messaging, often independently.[123] Therefore, many of the strategy proposals found throughout the discourse focused on unifying and integrating stakeholders to create a more coordinated response. Within the U.S. government, two primary agencies have mounted response efforts to combat disinformation, the DHS and the GEC. This section first explores how these two agencies coordinate now to combat deceptive messaging and then identifies the dominant discussions and recommendations for better coordination within the literature.

As of 2019, the GEC is the agency tasked with leading the U.S. government efforts to counter disinformation and propaganda.[124] Despite critics arguing that the GEC is ineffective, its mission was expanded in the National Defense Authorization Act for fiscal year 2019 to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal

---

[121] Lewsey.

[122] U.S. Senate Committee on Homeland Security and Governmental Affairs, "Peters, Portman Bill Responding to Growing Threat."

[123] Bodine-Baron et al., *Countering Russian Social Media Influence*, x.

[124] Department of State, "Global Engagement Center."

Government to recognize, understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts."[125] It is worth highlighting that the GEC is primarily focused outward on foreign entities and that domestic matters fall outside of its scope. Although the degree of coordination or integration with each stakeholder is not clear, the GEC claims to partner with the following government agencies:

- U.S. Agency for International Development (USAID)
- U.S. Agency for Global Media (USAGM)
- Department of State (DOS)
- Department of Justice (USDOJ)
- Department of Defense (DOD)
- National Counterterrorism Center (NCTC)
- Central Intelligence Agency (CIA)
- Department of Homeland Security (DHS)
- Department of Treasury (DOT)
- Small Business Administration (SBA)[126]

The GEC also claims to consult with "allied governments, non-governmental organizations (NGO), and civil society, as well as with private-sector experts."[127] Despite the GEC claiming to have relationships with a broad array of stakeholders, the extent of these coordination efforts appear to be consultations and partnerships, rather than a joint or integrated effort, and seem to lack a guiding framework or strategy.

---

[125] John S. McCain National Defense Authorization Act for Fiscal Year 2019.

[126] "About Us—Global Engagement Center," Department of State, accessed September 6, 2019, https://www.state.gov/about-us-global-engagement-center/.

[127] Department of State.

The DHS has also emerged as another leading agency to combat deceptive messaging. In an official report in May 2019, the HSAC formally recognized a gap in leadership and called upon the DHS to create "an inter-agency task force that would include all federal entities involved in countering the threat of FI [foreign influence]" and "play a leading role in raising public awareness efforts, ensuring effective coordination, and providing information sharing mechanisms to identify and help counteract foreign influence operations."[128] Although it is not clear how much progress has been made since the report was published, the DHS touts a Countering Foreign Influence Task Force (CFITF) that was established in 2018.[129] In his earlier testimony before Congress, Matthew Masterson, a CISA Senior Cybersecurity Advisor, indicates that CFITF has largely played a support role to CISA operations but has plans to expand in 2020.[130] The DHS CISA has taken significant strides to address foreign interference as part of the "Protect2020" campaign due to the threat it poses to election security.[131] Through this campaign, they have worked closely with federal, state, local, tribal, and territorial (FSLTT) agencies, election officials, private sector companies, and even published publicly available resources to engage the public.[132] While both the GEC and DHS seem

---

[128] Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*, 10.

[129] Cybersecurity and Infrastructure Security Agency, *#Protect2020 Strategic Plan* (Washington, DC: Department of Homeland Security, 2020), 4–16, https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan_FINAL%202.7.20%20508.pdf.

[130] *Testimony Matthew Masterson Senior Cybersecurity Advisor Cybersecurity and Infrastructure Security Agency U.S. Department of Homeland Security for a Hearing on Securing America's Elections Part II: Oversight of Government Agencies before the United States House of Representatives Committee on the Judiciary*, House of Representatives, 116th Cong., 1st sess., October 22, 2019, 5–6, https://www.congress.gov/116/meeting/house/110106/witnesses/HHRG-116-JU00-Wstate-MastersonM-20191022.pdf.

[131] Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Foreign Interference."

[132] H.R., *Testimony Matthew Masterson Senior Cybersecurity Advisor Cybersecurity and Infrastructure Security Agency U.S. Department of Homeland Security for a Hearing on Securing America's Elections Part II*, 1–3.

to be pursuing some degree of multi-stakeholder coordination efforts, critics find that more work needs to be done.

Throughout the literature, three overarching terms were used to describe the degree of coordination necessary to combat deceptive messaging: whole-of-society, whole-of-government, and whole-of-nation.[133] Although these terms seem to refer to a common goal of coordinating across a broad community of stakeholders, a clear definition of exactly which stakeholders each one includes or excludes is not readily apparent. Few authors took the time to define the scope of the phrase they used specifically when discussing the layers of coordination needed. Based on the information available, I outlined the specific stakeholder groups that should fall within each term.

Out of the many authors who employed one of the three terms, this author identified just two that clearly defined their use of it in the context of combatting deceptive messaging. Waltzman defines whole-of-nation as "a coordinated effort between national government organizations, military, intelligence community, industry, media, research organizations, academia and citizen organized groups."[134] Waltzman's definition is highly inclusive of entities within U.S. borders; however, it does not include international partners or allies. Despite this layer of coordination not being incorporated in his definition, he goes on to mention the need for cross-country coordination.[135] Similarly, Suzanne Spaulding calls for a whole-of-nation campaign and describes it as, "a national approach that pulls together governments, at all levels in the United States and with like-minded nations around the globe, along with civil society, academia, technology companies, and the public."[136] The primary differences between Waltzman's and Spaudling's definitions were

---

[133] Waltzman, *The Weaponization of Information*, 4–5; Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 17–22; Warner, "A New Doctrine for Cyberwarfare & Information Operations."

[134] Waltzman, 4–5.

[135] Waltzman, 4–5.

[136] Suzanne Spaulding and Eric Goldstein, *Countering Adversary Threats to Democratic Institutions* (Washington, DC: Center for Strategic and International Studies, 2018), V, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180214_Spaulding_CounteringAdversaryThreats_Web2.pdf?EzqGtMwOAjQIIH8eRNNoZ10T49OV63lh.

that Waltzman omitted the public and international partners; however, he still discussed these two elements and incorporated them into his research.[137]

Not all authors chose to use the term whole-of-nation in their research. Mark Warner argued, "we need not just a whole-of-government approach; we need a whole-of-society cyber doctrine."[138] Without specifically defining what the difference is between whole-of-government and whole-of-society, he goes on to discuss the need for the government to work with international allies, the private sector, and the American public.[139] His argument indicates that he views whole-of-society as a much more comprehensive form of coordination compared to whole-of-government. Fly, Rosenberger, and Salvo take a different approach and called for both a whole-of-government approach, focused on bridging all levels of government, and a whole-of-society approach, focused on the integration of civil society and the private sector.[140] In both reports, whole-of-society was a more inclusive term than whole-of-government, and is better aligned with the needs identified in the strategy recommendations.

After a comparison across the literature, the terms "whole-of-society" and "whole-of-nation" seem to be largely synonymous and also include the most variety of relevant stakeholders. Understanding the different layers of coordination and types of stakeholders each term signifies will be critical to strategy development to ensure a crucial partner is not overlooked. For example, the HSAC used the term whole-of-society in its official report for the DHS that stated, "it is critical to develop a whole-of-society approach where government agencies have a meaningful liaison with the private sector, media, technology companies, academia, think tanks, and the general public."[141] Based on the use and

---

[137] Waltzman, *The Weaponization of Information*, 4–5.

[138] Warner, "A New Doctrine for Cyberwarfare & Information Operations."

[139] Warner.

[140] Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 17–22.

[141] Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*, 10.

definitions of the three terms found within the literature, Table 1 visually compares and contrasts the stakeholders included within each of the three terms.

Table 1. Coordination Terminology

Stakeholder	Whole-of-Society	Whole-of-Government	Whole-of-Nation
Federal, state, and local government	**X**	**X**	**X**
Private Sector	**X**		**X**
Civil Society and Non-Governmental Organizations	**X**		**X**
Academia	**X**		**X**
The Public	**X**		**X**
International Allies	**X**		**X**

Scholars and critics of government coordination efforts have translated the terminology used into more specific coordination models that describe what a multi-stakeholder effort may look like and how it could operate. Deeks, McCubbin, and Poplin proposed using the Active Measures Working Group (AMWG) from the Soviet era, as a potential interagency model that includes participants from the government, private sector, and academia.[142] The AMWG was regarded as a successful interagency committee that

[142] Deeks, McCubbin, and Poplin, "Addressing Russian Influence."

comprised a range of experts from all levels of government.[143] The AMWG "exposed some Soviet covert operations and raised the political cost of others by sensitizing foreign and domestic audiences to how they were being duped."[144] The AMWG was more closely aligned with a whole-of-government approach; however, an updated version of this model to incorporate other partners, as noted by Deeks, McCubbin, and Poplin, would be more aligned with a whole-of-nation or whole-of-society approach.[145] Bodine-Baron et al. support their recommendation and expand on it by highlighting that the AMWG-like committee should be independent.[146] The AMWG-like model was just one suggestion aimed at integrating stakeholders.

However, not all scholars agree that an AMWG-like committee would be as successful today as it was in the 1980s. Schoen and Lamb argue that although the AMWG was successful, it would be difficult to duplicate.[147] They support their argument by claiming that interagency missions are so broad and it would be challenging to find exceptional leaders who would protect the group mission versus the lead agency's mission to achieve a similar result or effectiveness seen in the 1980s.[148] Schoen and Lamb's research, however, goes on to highlight the factors for success, challenges, and inner workings of U.S. government interagency groups.[149] Such research will likely be valuable as other authors also explored other interagency solutions to the coordination challenge.

---

[143] Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Strategic Perspectives no. 11 (Washington, DC: Institute for National Strategic Studies, 2012), 1, https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

[144] Schoen and Lamb, 168.

[145] Deeks, McCubbin, and Poplin, "Addressing Russian Influence."

[146] Bodine-Baron et al., *Countering Russian Social Media Influence*, 43–44.

[147] Schoen and Lamb, *Deception, Disinformation, and Strategic Communications*, 5.

[148] Schoen and Lamb, 115–120.

[149] Schoen and Lamb, 8–97.

Fried and Polyakova recommended a fusion cell modeled after the NCTC along with an international "counter-disinformation coalition" as another possible approach.[150] The NCTC is a whole-of-government model that comprises employees from a wide variety of government organizations.[151] Just like the current model, Fried and Polyakova suggest that a "'national counter-disinformation center' would include representatives from the Federal Bureau of Investigation (FBI), the Central Intelligence Agency, the aforementioned DHS information coordination office, the Department of Defense, the GEC, and other relevant agencies."[152] In later research, they add that this center should have "a mandate for real-time liaison with foreign governments, social media companies, civil society, and other relevant actors."[153] The NCTC model is very similar to the AMWG-like model, which seeks to build a group of interagency participants. However, not all scholars agree that this approach will be successful.

Farwell is skeptical of the NCTC model for similar reasons cited by Schoen and Lamb about the AMWG-like concept.[154] Farwell argues, "the most challenging aspect of this approach involves relying exclusively on government expertise...information warfare requires a wide range of outside experts—many with unconventional skills."[155] Although skeptical of the NCTC suggestion, Farwell supports a team of teams concept because it "can capitalize on the strengths of all elements of national power to achieve its objectives and leverage the power of the presidency to maximize them."[156] Stanley McChrystal used the team of teams approach as a method to create highly effective teams that operate as a

---

[150] Fried and Polyakova, *Democratic Defense against Disinformation*, 6–7; Polyakova and Fried, *Democratic Defense against Disinformation 2.0*, 16.

[151] "Partnerships," National Counterterrorism Center, accessed September 2, 2019, https://www.dni.gov/index.php/nctc-how-we-work/partnerships.

[152] Fried and Polyakova, *Democratic Defense against Disinformation*, 6–7.

[153] Polyakova and Fried, *Democratic Defense against Disinformation 2.0*, 16.

[154] Farwell, "Countering Russian Meddling in U.S. Political Processes," 41.

[155] Farwell, 41.

[156] Farwell, 41.

network, rather than in a hierarchy or bureaucracy, to combat terrorist networks in Iraq.[157] While the AMWG, NCTC, and team of teams models all seek to achieve a highly integrated and effective team focused on combating deceptive messaging, the authors have made it clear that doing so will be challenging and that U.S. government leaders must put a lot of consideration into the creation of any task force or committee to ensure the group dynamics provide effective and positive results.

The strategy recommendations made for coordination outlined ways in which the U.S. government can improve its efforts to fight deceptive messaging. However, integrating public-private sector entities, as Nathan Busch and Austen Givens explain, presents "significant implications for management practices, legal and ethical challenges, transparency, building private sector participation, politics, budgeting, and long-term planning;" it is no easy feat.[158] In support of Busch and Givens, Bodine-Baron et al. also point out that private sector companies will likely be reluctant to cooperate with the government, "especially in terms of sharing proprietary data, private data, or both."[159] Speaking from professional experience; however, some private sector agencies are motivated to share information as it pertains to public safety and national security with government agencies once trust and a clearly defined process can be established. Due to the challenges of such broad integration, as well as the apparent importance of comprehensive coordination as a foundation for almost every aspect of combating deceptive messaging, the following chapters focus on how the U.S. government can start coordinating more effectively with different groups of stakeholders.

---

[157] Stanley A. McChrystal et al., *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin Publishing Group, 2015), loc. 21–64 of 6029, Kindle.

[158] Nathan E. Busch and Austen D. Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," *Homeland Security Affairs* 8, art. 8 (October 2012), https://www.hsaj.org/articles/233.

[159] Bodine-Baron et al., *Countering Russian Social Media Influence*, 44.

III. GOVERNMENT COORDINATION IN PRACTICE

Without a guiding strategy or framework, the U.S. government appears not to have a clear path forward for building the level of coordination that experts call for; therefore, it is worth leveraging information garnered from existing practices. The EU's fight against disinformation is just one case from which the United States can learn. In her earlier testimony before Congress, Polyakova stated, "The United States has fallen behind Europe in both conceptualizing the nature of the challenges and operationalizing concrete steps to counter and build resilience against disinformation."[160]

European democracies have been the targets of foreign influence and deceptive messaging operations and threats longer than the United States. They therefore had more time to develop a more practical knowledge to respond to them.[161] The EU began a multilateral, joint response to fight disinformation in 2015 that supports and coordinates across member states.[162] It has been incrementally building and evolving the response ever since.[163] Additionally, the United States is an EU ally and shares similar democratic values, which makes the sharing and application of smart practices less complicated. U.S. government leaders could leverage the EU's knowledge about its mistakes, challenges, and successes specific to coordination in its response to disinformation to accelerate the development of a whole-of-society approach in America.

---

[160] H.R., *United States House Committee on Appropriations—Subcommittee on State, Foreign Operations, and Related Programs United States Efforts to Counter Russian Disinformation and Malign Influence*.

[161] Margaret L. Taylor, "Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe," *Techtank* (blog), July 31, 2019, https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

[162] European Commission, *Action Plan against Disinformation: Report on Progress* (Brussels: European Commission, 2019), 1, https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf.

[163] European Commission, 1.

A. THE EUROPEAN UNION'S JOINT AND COORDINATED ACTION AGAINST DISINFORMATION

Government leadership in the EU consistently promoted the importance of coordination for its response to disinformation, which made it a central component of the EU's response. The European Council called for an action plan "with specific proposals for a coordinated response to the challenge of disinformation, including appropriate mandates and sufficient resources."[164] The top-down messaging was powerful and provided agencies with the latitude to use necessary resources for coordination measures that frame the response, which are highlighted as follows. Nevertheless, coordination is just a small piece of a more robust response from the EU.

This robust response has been captured in several publicly available documents and progress reports that detail the EU's approach to disinformation since 2015. Although not an exhaustive list of actions, the primary documents that frame the EU's response are the following:

- *Joint Framework on Countering Hybrid Threats*, April 2016[165]
- *Communication on Tackling Online Disinformation: A European Approach*, April 2018[166]

---

[164] European Commission, *European Commission Contribution to the European Council: Action Plan against Disinformation* (Brussels: European Commission, 2018), 1, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

[165] European Commission, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats* (Brussels: European Commission, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en.

[166] European Commission, *Communication from the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling Online Disinformation: A European Approach* (Brussels: European Commission, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN.

- *Report from the Commission on the Implementation of the Communication "Tackling Online Disinformation: A European Approach,"* December 2018[167]

- *EU Code of Practice on Disinformation*, September 2018[168]
  - Code of Practice monthly reports, January 2019 and ongoing[169]
- *Action Plan against Disinformation*, December 2018[170]
  - *Report on the Implementation of the Action Plan Against Disinformation*, June 2019[171]

Each of these reports illustrates the evolution of the EU's response over the past several years, and complements one another. The full timeline of the response can be traced back to a European Council meeting in March 2015, in which it concluded that the establishment of a communication team was the first step to challenge Russia's disinformation campaigns.[172] That communication team is known as the East StratCom Task Force, which is discussed in further detail in the following sections.[173] The *Joint*

---

[167] European Commission, *Report from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the Implementation of the Communication: "Tacking Online Disinformation: A European Approach,"* (Brussels: European Commission, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0794&from=EN.

[168] European Commission, *EU Code of Practice on Disinformation* (Brussels: European Commission, 2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

[169] European Commission, "Code of Practice on Disinformation."

[170] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation* (Brussels: European Commission, 2018), https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation.

[171] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the Implementation of the Action Plan against Disinformation* (Brussels: European Commission, 2019), https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

[172] General Secretariat of the Council, *European Council Meeting (19 and 20 March 2015)–Conclusions*, EUCO 11/15 (Brussels: European Council, 2015), 5, https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.

[173] "Questions and Answers about the East StratCom Task Force," European External Action Service, European Commission, May 12, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

Framework on Countering Hybrid Threats, a broad initiative to reinvent the EU's response to emerging security threats, expands on strategic communication improvements to fight disinformation.[174] The joint framework also calls for the East StratCom Task Force to improve its capabilities by incorporating "linguists fluent in non-EU languages and social media specialists."[175]

Expanding its approach to disinformation in the *Communication on Tackling Online Disinformation*, the EU defines the threat and "outlines the key overarching principles and objectives which should guide actions to raise public awareness about disinformation and tackle the phenomenon effectively."[176] The report organizes objectives under the following overarching principles: transparency of online platforms, strengthening fact-checking, fostering accountability, harnessing new technologies, securing elections, "fostering education and media literacy, supporting quality journalism, and countering disinformation through strategic communication."[177] This report also lays the foundation for the development of the *EU Code of Practice on Disinformation* and the *Action Plan against Disinformation*, which build on the initial concepts in the *Communication on Tackling Online Disinformation.*[178] Figure 1 illustrates this evolution and iteration of the EU's response to disinformation across a timeline.

---

[174] European Commission, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats.*

[175] European Commission, 5.

[176] European Commission, *Report from the Commission...Tackling Online Disinformation*, 3.

[177] European Commission, 7–16.

[178] European Commission, 2–7.

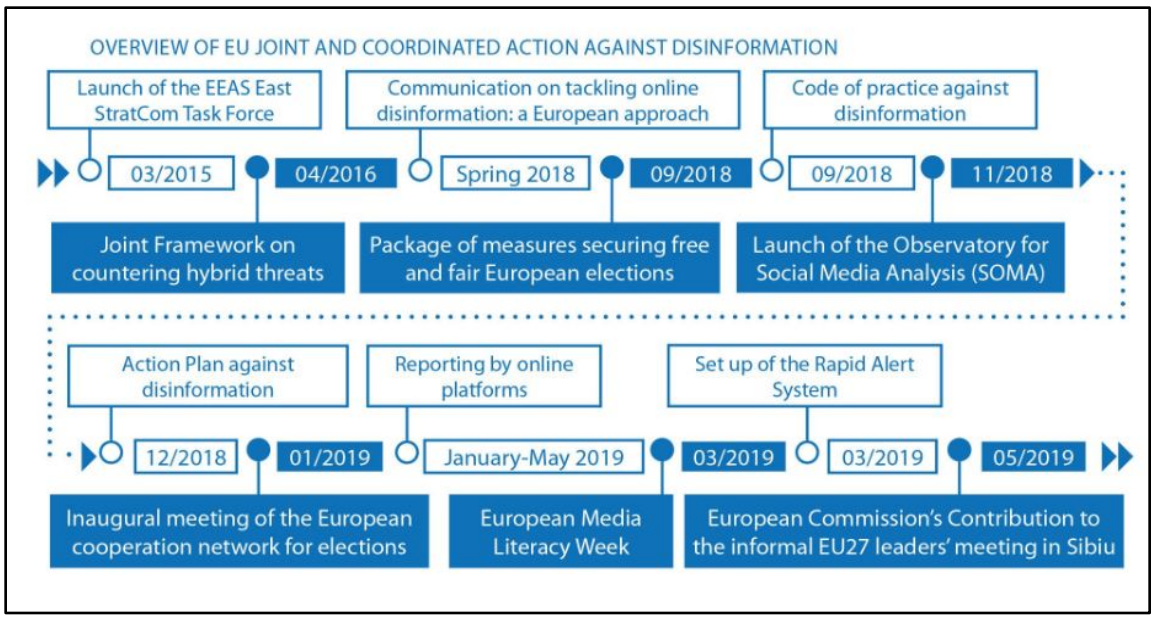

Figure 1. Overview of EU Joint and Coordinated Action against Disinformation.[179]

In the early years of the response, the East StratCom Task Force was one of the first steps towards coordination that EU institutions took to respond to disinformation.[180] The task force itself is an effort of coordination because it comprises 16 positions filled by EU institutions or member states.[181] Additionally, it, "leads a myth-busting network that comprises over 400 experts, journalists, officials, NGOs and think tanks operating in more than 30 countries," and "works closely with the EU institutions, EU Delegations, Member States, and a wide range of other partners, both governmental and non-governmental, within the EU, in the Eastern Neighbourhood, and beyond."[182] The purpose of the task force's extensive collaboration is to "share best practices in strategic communications and access to objective information, and to ensure support for independent media in the

[179] Source: European Commission, "Tackling Online Disinformation."

[180] European Commission.

[181] European External Action Service, "Questions and Answers about the East StratCom Task Force."

[182] De Jong et al., *Inside the Kremlin House of Mirrors*, 12; European External Action Service.

region."[183] In 2018, the Foreign Affairs Council commended the East StratCom Task Force for its efforts in strengthening the resilience of the EU and its neighbors against Russian threats.[184] The East StratCom Task Force is just one of many other coordination efforts in the EU response to disinformation.

To enhance coordination with the private sector, the European Commission published the *EU Code of Practice on Disinformation* in September 2018.[185] The code establishes strategic relationships with the private sector, particularly online platforms and advertising companies, through a voluntary agreement that allows for indirect government regulation.[186] The purpose of it is "to identify the actions that Signatories could put in place in order to address the challenges related to 'Disinformation'"[187] Signatories include Twitter, Google, Facebook, Mozilla, and advertisers and advertising industry.[188] This agreement first institutes a common definition of disinformation that aligns with the rest of the EU's response efforts and sets commitments for the signatories surrounding the scrutiny of ad placements, political advertising and issue-based advertising, integrity of services, empowering consumers, empowering the research community, and measuring and monitoring the code's effectiveness.[189] The code even goes as far as identifying best practices that signatories can apply to achieve their commitments.[190] To assess these commitments, signatories are required to submit monthly progress reports for the European Commission to conduct targeted monitoring of progress and compliance.[191] Iva Plasilova

---

[183] European External Action Service.

[184] Council of the European Union, *Outcome of the Council Meeting, 3613rd Council Meeting, Foreign Affairs, Luxembourg, 16April2018* (Brussels: Press, 2018), 3, https://www.consilium.europa.eu/media/33743/st07997-en18.pdf.

[185] European Commission, *EU Code of Practice on Disinformation*.

[186] European Commission.

[187] European Commission, 3.

[188] European Commission, "Code of Practice on Disinformation."

[189] European Commission, *EU Code of Practice on Disinformation*.

[190] European Commission, 2.

[191] European Commission, "Code of Practice on Disinformation."

et al. assessed the Code of Practice in 2020 and determined that there is still room for improvement on items, such as enforcement, but concluded, "the Code should not be abandoned" because it "has established a common framework" and "has produced positive results."[192] In addition to task forces and formal agreements, the EU has also achieved better coordination through other activities, such as information-sharing initiatives.

The Rapid Alert System, a digital platform for information sharing, also resulted in better coordination among stakeholders.[193] The platform connects 28 government coordinators of EU institutions or member states who can share instances of disinformation campaigns, analysis, trends, reports, and best practices in real-time.[194] The dedicated mechanism for information sharing has increased the interactions and coordination among EU institutions, member states, national authorities, the North Atlantic Treaty Organization (NATO), the Group of Seven (G7), and online platforms since its implementation in March 2019.[195] Regardless of the system's success, it has already paid dividends in building relationships between disinformation experts in the region that can outlive the system. Such relationship building can take time, and the interactions resulting from the system represent a significant milestone in forward progress toward that end.

Although the EU has made progress with the three highlighted initiatives, its coordination efforts are not perfect, and it has struggled with scaling its response and obtaining an acceptable level of private-sector participation. The EU has publicly addressed these challenges and developed solutions to resolve them. In 2017, De Jong et al. pointed out that the East StratCom Task Force activities were small compared with the propaganda produced by Russia, and cited the lack of budget and staffing as part of the

---

[192] Iva Plasilova et al., *Study for the "Assessment of the implementation of the Code of Practice on Disinformation* (Luxembourg: Publications Office of the European Union, 2020), 3–5, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66649.

[193] European Union External Action, *Rapid Alert System Strengthening Coordinated and Joint Responses to Disinformation* (Brussels: European Union External Action, 2019), 1, https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.

[194] European Union External Action, 1.

[195] European Commission, *Joint Communication...Report on the Implementation of the Action Plan against Disinformation*, 1–9.

challenge.[196] Since then, the EU has made strides to increase the scale of the task force's efforts by stating that the budget supporting the task force, among other groups, is expected to more than double "from €1.9 million in 2018 to €5 million in 2019."[197] In addition to budget challenges, the signatories of the Code of Practice have been slow to include valuable details in their monthly progress reports about disinformation on their platforms.[198] As a result, the commission has publicly urged them to step up their efforts on multiple occasions.[199] The signatories have since agreed to "improve the transparency, accountability and trustworthiness of their services."[200] These illustrations are two examples of how the EU has worked to improve its weaknesses and mature its response. The strengths and weaknesses of the EU's approach to coordination offer key lessons and best practices that can be applied to U.S. efforts to mitigate deceptive messaging.

B. LESSONS LEARNED AND SMART PRACTICES

The EU's response to disinformation has demonstrated many invaluable lessons with regard to coordination for the United States. The East StratCom Task Force, the *EU Code of Practice on Disinformation*, and the Rapid Alert System all present ideas in which the United States can use to coordinate across government, the private sector, international allies and institutions, academia, and civil society better to combat deceptive messaging. Besides key takeaways from those three examples, the United States should also consider other elements of the EU's response that may also facilitate effective coordination and other strategic goals. Other considerations for application in the United States include the top-down driven strategy development, the availability and accessibility of information, and the emphasis on citizen engagement.

---

[196] De Jong et al., *Inside the Kremlin House of Mirrors*, 14.

[197] European Commission, *Fact Sheet—Questions and Answers—The EU Steps Up Action against Disinformation* (Brussels: European Commission, 2018), 2, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_18_6648/MEMO_18_6648_EN.pdf.

[198] European Commission, *Joint Communication...Report on the Implementation of the Action Plan against Disinformation*, 4–5.

[199] European Commission, 4.

[200] European Commission, 4.

The support and leadership of European Commission and European Council throughout the development of the EU's response to disinformation was beneficial in many ways.[201] First, it meant that the actions taken by EU institutions, such as the creation of the East StratCom Task Force, were supported and encouraged by top government leadership. Such support is important for obtaining resources needed to develop and execute coordination efforts. Second, political leaders could hold government institutions and other stakeholders accountable to the quality of their work and the tempo of development. The use of hard deadlines was prevalent throughout the material. For example, the European Council invited the High Representative and the Commission to present "an action plan by December 2018."[202] Third, political leaders could broadly communicate such initiatives and have greater influence over other relevant stakeholders within and outside the government, which helps to garner more participation and cooperation in the response. In addition to the overall development of the plan, the commission also recognized the need for public awareness and access to information.[203]

The availability of official reports and an emphasis on public engagement throughout the EU response to disinformation have been praiseworthy and may be valuable for facilitating coordination efforts with the public and other stakeholders in the United States. Throughout this research, official reports from EU institutions about the response were often the top search results on search engines and were easily found. Whether or not the EU has something to do with the searchability of its information, it is important because if credible information about deceptive messaging or the government's response efforts cannot be easily found, people may resort to sources of questionable credibility that are easier to find. Additionally, the information about the response is consistently updated on public websites and often includes dates for when the next update or report will be published. Once published, many of the reports were released in many different languages. For instance, the *Joint Framework on Countering Hybrid Threats* was published in at least

---

[201] European Commission, *Joint Communication... Action Plan against Disinformation*.

[202] European Commission, 1.

[203] European Commission, 9–11.

23 different languages.[204] Although the United States does not comprise different countries with unique languages or dialects, as the EU does, the United States Census Bureau reported in 2015 that there are "at least 350 languages spoken in U.S. homes."[205] If reports are published only in English, non-native speakers are precluded from access to the information and must rely on other sources that may be less credible. This emphasis on the importance of EU citizens was established in the first few sentences of the *Action Plan against Disinformation*, "European democracy is only as strong as the active participation of its citizens."[206] This fundamental mindset prompted many of the above public engagement measures throughout the response. The qualities of a top-down approach, information availability, and public engagement have presented more opportunities for coordination with stakeholders outside the government and the public.

In contrast, the U.S. government should cautiously consider and evaluate some aspects of the EU response. One example is the heavy focus on Russian disinformation activity throughout the EU's response.[207] Since the EU recognizes that the "Russian Federation poses the greatest threat to the EU," this emphasis on Russia seems appropriate.[208] Russia also poses a significant threat to the United States; however, it may also be susceptible to harmful deceptive messaging from other nefarious actors other than Russia. The EU does briefly recognize other state, non-state, and domestic actors in the problem space; however, minimizing them in the United States could create weaknesses for a national-level response.[209] The EU model will not have all the answers for the

---

[204] "Joint Communication to the European Parliament and the Council Joint Framework on Countering Hybrid Threats a European Union Response," European Commission, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

[205] "Census Bureau Report at Least 350 Languages Spoken in U.S. Homes," United States Census Bureau, November 3, 2015, https://www.census.gov/newsroom/press-releases/2015/cb15-185.html.

[206] European Commission, *Joint Communication... Action Plan against Disinformation*.

[207] European Commission, 2–5.

[208] European Commission, 4.

[209] European Commission, 3–4.

development of a United States response; however, the positives and negatives about it provide many insights.

While the EU's response model to disinformation may not be perfect, the United States can leverage both the positive and negative aspects of it to accelerate its coordination efforts at home. It should be noted that coordination is just a small piece of a more comprehensive approach in the EU, and more components may be worth examining further, such as public resilience and the policy and regulation measures discussed in Chapter II. Despite the value that the EU's experience offers, the U.S. government will need to develop an implementation plan for coordination specific to its stakeholders. Therefore, Chapter IV presents collective impact as a tool that U.S. government leaders can use to build relationships with stakeholders across different sectors to address the deceptive messaging threat in a more unified and cohesive manner.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COLLECTIVE IMPACT: A ROADMAP FOR COORDINATION

The EU case study provides valuable insight into the role of coordination in its response to disinformation; however, it does not explicitly identify the steps that must be taken to build a disinformation task force or a connected network of stakeholders that have a wide variety of missions, budgets, goals, and expectations. As identified in Chapter II, the establishment of any organization to combat deceptive messaging in the United States must be done strategically and thoughtfully to foster effective and efficient relationships across stakeholders within and outside of the government. Such coordination is no easy task, and scholars are quick to point out the many failures of similar coordination attempts in U.S. history. Therefore, U.S. government leaders still need an implementation plan for adopting and executing any of the proposed coordination models.

Since coordination across a broad range of stakeholders is not a new challenge, tools and frameworks, with proven success, are available that can facilitate the process. Collective impact is one method that has been used to facilitate the development of coordination between stakeholders across different sectors to solve complex problems that vary in magnitude and type.[210] For example, collective impact brought together all the stakeholders that comprise the New York State (NYS) Juvenile Justice System in 2011 to address inefficiencies and failures.[211] Despite each stakeholder having a different mission, scope, or budget, the sustained coordination through the collective impact method brought measurable success to a failing system.[212] This case is explored in further detail later in this chapter. Additionally, when reviewed closely, the elements needed for collective

---

[210] John Kania and Mark Kramer, "Collective Impact," *Stanford Social Innovation Review* 9, no. 1 (Winter 2011): 36–41, https://ssir.org/articles/entry/collective_impact; Jewlya Lynn et al., *When Collective Impact Has an Impact: A Cross-Site Study of 25 Collective Impact Initiatives* (Seattle, WA: ORS Impact, 2018), 17, https://www.orsimpact.com/DirectoryAttachments/10262018_111513_477_CI_Study_Report_10-26-2018.pdf.

[211] New York State Juvenile Justice Advisory Group, *New York State Juvenile Justice: Progress toward System Excellence* (Boston, MA: FGS, 2014), 1–4, https://www.collectiveimpactforum.org/sites/default/files/NYS_Juvenile_Justice_Progress_Report_0.pdf.

[212] New York State Juvenile Justice Advisory Group, 1–4.

impact exist throughout the EU response to disinformation. Due to the positive examples and alignment with the needs for coordination, this chapter introduces and assesses collective impact as an option for building a whole-of-society response to deceptive messaging in American society.

A. THE CONDITIONS OF IMPACT

The level of coordination that exists across stakeholders combating deceptive messaging is a patchwork of ad hoc partnerships and collaborations that fall short. Collective impact is a more structured and comprehensive approach to coordination designed to bring together and align all relevant stakeholders around a centralized framework.[213] John Kania and Mark Kramer define collective impact initiatives as, "long-term commitments by a group of important actors from different sectors to a common agenda for solving a specific social problem. Their actions are supported by a shared measurement system, mutually reinforcing activities, and ongoing communication, and are staffed by an independent backbone organization."[214] By centralizing and focusing stakeholders' efforts to combat deceptive messaging with a common agenda, the government can reduce the duplication of effort, maximize resources toward a desired outcome, and leverage special or unique skill sets.

True alignment of stakeholders will rely on achieving all five conditions of collective impact:

- common agenda
- shared measurement
- mutually reinforcing activities
- continuous communication

---

[213] Kania and Kramer, "Collective Impact," 39.

[214] Kania and Kramer, 39.

- backbone support[215]

The foundation of the framework starts with the common agenda, or guiding strategic plan and vision supported and reinforced by the other four conditions.[216] Shared measurement establishes a method for benchmarking progress, mutually reinforcing activities ensures that action and efforts are methodical and organized, continuous communication to strengthen the relationships between stakeholders needed to make any of the other conditions successful, and backbone support provides administrative oversight of the entire operation to bolster the efforts of stakeholders.[217] Each condition is highly interdependent, and if all five are not fulfilled, the chances for success are unlikely. The five conditions of collective impact are defined in more detail in Table 2.

[215] Kania and Kramer, 41.

[216] Kania and Kramer, 39–41.

[217] Kania and Kramer, 39–41.

Table 2. The Five Conditions of Collective Impact.[218]

The Five Conditions of Collective Impact

Common Agenda	All participants share a vision for change that includes a common understanding of the problem and a joint approach to solving the problem through agreed-upon actions.
Shared Measurement	All participating organizations agree on the ways success will be measured and reported, with a short list of common indicators identified and used for learning and improvement.
Mutually Reinforcing Activities	A diverse set of stakeholders, typically across sectors, coordinate a set of differentiated activities through a mutually reinforcing plan of action.
Continuous Communication	All players engage in frequent and structured open communication to build trust, assure mutual objectives, and create common motivation.
Backbone Support	An independent, funded staff dedicated to the initiative provides ongoing support by guiding the initiative's vision and strategy, supporting aligned activities, establishing shared measurement practices, building public will, advancing policy, and mobilizing resources.

To fulfill each condition, a large volume of resources and tools are available to facilitate and improve collective impact initiatives. The five phases of collective impact is one resource available to provide a roadmap for practitioners combating deceptive messaging.[219] These phases were identified and refined because of experience and research from practitioners actively engaged with collective impact initiatives.[220] The five phases include:

- generate ideas and host dialogues
- initiate action

---

218 Source: John Kania, Fay Hanleybrown, and Jennifer Splansky Juster, "Essential Mindset Shifts for Collective Impact," *Stanford Social Innovation Review* 12, no. 4 (Fall 2014): 2, https://ssir.org/articles/entry/essential_mindset_shifts_for_collective_impact.

219 Tamarack Institute, *Collective Impact Self-Assessment and Planning Tool* (Waterloo, ON: Tamarack Institute, 2017), 1, https://www.tamarackcommunity.ca/hubfs/Collective%20Impact/Tools/CI%20Self%20Assessment%20Tool.pdf?hsCtaTracking=8df74891-21af-4a7c-88d7-bb024f0d7d62%7C90f5999e-f7d9-4112-890e-96ed8a56a460.

220 "Collective Impact," Tamarack Institute, accessed September 12, 2020, https://www.tamarackcommunity.ca/collectiveimpact.

- organize for impact
- begin implementation
- sustain action and impact[221]

The phases of collective impact are similar to the overarching timeline of a large project or business, starting with exploration and start-up that evolves into implementation, refinement, and sustainment.[222] The five phases, seen in Figure 2, provide a roadmap for practitioners to identify where they are in the collective impact process and it also helps them understand what their next steps should be to fulfill the five conditions.

Within each phase, key milestones or actions are organized across the four components of an initiative:

- governance and infrastructure
- strategic planning
- community engagement
- evaluation and improvement[223]

Each component is focused on a specific goal that ultimately fulfills one or more conditions of collective impact. For example, the goal of governance and infrastructure is "to agree upon how your initiative is best designed and led."[224] The key milestones within governance and infrastructure result in the eventual development of a backbone organization.[225] By using the phases of collective impact, practitioners can visualize the necessary steps to fulfill all five conditions, and stay organized and focused for maximum

---

[221] Tamarack Institute, *Collective Impact Self-Assessment and Planning Tool*, 2.

[222] Tamarack Institute, 2.

[223] Tamarack Institute, 2.

[224] Tamarack Institute, 3.

[225] Tamarack Institute, 2.

efficiency. This resource can accelerate the development of a plan specific to deceptive messaging stakeholders by using lessons learned from previous initiatives to reduce inefficiencies or time spent troubleshooting challenges. The five phases, components of success, and key milestones are illustrated in Figure 2.

The Phases of Collective Impact						
Over-arching Actions	Components of Success	Phase I *Generate Ideas and Host Dialogues*	Phase II *Initiate Action*	Phase III *Organize for Impact*	Phase IV *Begin Implementation*	Phase V *Sustain Action & Impact*
		Pre-Start-up *Focus: Engagement and Exploration*	**Start-up** *Focus: From Idea to Formation*	**Foundation Building** *Focus: A container to work collectively*	**Growth** *Focus: Experimentation & Growth*	**Maturity** *Focus: Sustain & Renew*
		EARLY YEARS Key Questions: *What needs to happen? What structures do we need to work collectively to make it happen?*			**MIDDLE YEARS** Key Questions: *How well is it working?* What else is needed?	**LATER YEARS** Key Questions: *What difference are we making? How is our work sustained?*
		KEY ELEMENTS				
Design, Implement and Lead your CI Initiative	**Governance & Infrastructure** How decisions are made and responsibilities shared	Convene Community Leaders & Stakeholders	Identify champions and form cross-sector Steering Committee	Develop Initial CI infrastructure (backbone, Steering Committee & working groups)	Launch Working Groups and confirm Backbone Organization	Facilitate, refine and renew action plan and evolve structure
	Strategic Planning What are we trying to do and how: Our Theory of Change	Hold dialogue about issue, community context and available resources	Map the landscape and use data to make the case (develop implementation plan)	Create common agenda, community aspiration, understanding of the problem/opportunity & shared overall goal	Develop Implementation Blueprint and Initial Action Plan that identifies quick wins	Refine strategies and mobilize for quick wins. Review progress and determine renewal strategies
Understand Context	**Community Involvement** Who is involved? Who else's eyes need to be on this issue?	Assess community readiness & create plan for authentic community engagement	Begin community outreach, engage leaders	Broaden perspectives engaged. Emphasize *unusual suspects* & *passionate amateurs*	Continue engagement to build broad community will & shared ownership	Continue engagement & advocacy. Address opportunities to change policy
Assess Progress, Outcomes, Impact and Learning	**Evaluation & Improvement** What are we learning and how are we changing culture, norms and systems?	Determine if there is consensus and urgency to move forward	Analyze baseline data to ID key issues and gaps	Analyze baseline data to ID key issues & groups	Establish shared metrics (indicators, measurement and approach)	Collect, track, and report progress (process to learn, improve, and renew)

Figure 2. The Phases of Collective Impact.[226]

True alignment and agreement among stakeholders through all five conditions of collective impact, using the five phases as a guide, can amplify response efforts, and maximize the limited resources of each stakeholder to make it a worthwhile consideration to use in building a whole-of-society response to the deceptive messaging threat. For example, one collective impact initiative called Strive, which focuses on the success of children, "has a $1.5 million annual budget but is coordinating the efforts and increasing

[226] Source: Liz Weaver, "Navigating Collective Impact," *FSG* (blog), May 7, 2013, https://www.fsg.org/blog/navigating-collective-impact.

the effectiveness of organizations with combined budgets of $7 billion."[227] Budget limitations are a constant constraint for the U.S. government, and aligning resources towards common objectives with other stakeholders to leverage the resources of many is a creative step to bypass such challenges and develop a more lean operation.

Despite research showing that the collective impact model has "undoubtedly contributed to changes," it has some potential limitations.[228] In parallel with earlier discussions about the limitations of an AMWG-like model, Thaddeus Ferber and Erin White point out that government decision makers typically operate in such a way that results in "loyalty to a specific issue and funding stream," which is counterproductive to the collective impact method.[229] Joao Gomes, Marco Grotteria, and Jessica Wachter, echo this sentiment and state that the government needs a cultural shift "towards a focus on the bigger picture and overall impact of programs, rather than looking to short-term achievements as metrics of success."[230] The narrow focus and siloed culture of government was cited as a primary weakness of the intelligence community before the 9/11 terrorist attacks.[231] The priorities of each agency must be aligned with the broader group of stakeholders and the shared agenda to benefit the overall response rather than just one agency.

In addition to government culture, other potential limitations of collective impact include the amount of time it could take to see measurable results and the ability for

---

[227] Kania and Kramer, "Collective Impact," 41.

[228] Sarah Stachowiak and Lauren Gase, "Does Collective Impact Really Make an Impact?" *Stanford Social Innovation Review*, August 2018, https://ssir.org/articles/entry/does_collective_impact_really_make_an_impact.

[229] Thaddeus Ferber and Erin White, "Making Public Policy Collective Impact Friendly," *Stanford Innovation Review* 12, no. 4 (Fall 2014): 22, https://ssir.org/pdf/Fall_2014_Making_Public_Policy_Collective_Impact_Friendly.pdf.

[230] Michelle Lu, *Collective Impact in Promise Zones* (Philadelphia: Wharton, University of Pennsylvania, 2018), https://publicpolicy.wharton.upenn.edu/live/news/2674-collective-impact-in-promise-zones.

[231] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004), 416–419.

initiatives to endure changes in leadership. The NYS Juvenile Justice System saw results in just two years; however, one study of eight initiatives found that it could take anywhere from four to 24 years to see results.[232] These limitations of collective impact can, however, be mitigated through a variety of means.

Entire communities and consulting businesses are dedicated to support and improve collective impact initiatives.[233] Ferber and White conducted extensive research on creating successful collective impact initiatives within the government and identified a number of approaches and ideas to mitigate potential challenges.[234] Some of their suggestions included culture changes, such as, "creating interagency structures focused on populations and issues, flipping accountability from 'services provided' to 'outcomes achieved', and changing government auditing and accounting practices."[235] In addition to those three suggestions, Ferber and White also identified public policies across all five conditions that incentivize and encourage a collective impact in government. Some of the policies include funding, the development of requirements for funding and collaboration, and data-sharing agreements.[236] Without incentives driving the fulfillment of the conditions, participation in the initiative may not be strong or sustainable and competing priorities may detract the attention of stakeholders. All the suggested public policies to drive or incentivize collective impact for each condition are shown in Table 3.

---

[232] Kania and Kramer, "Collective Impact," 35.

[233] Hallie Preskill, Marcie Parkhurst, and Jennifer Splansky Juster, *Guide to Evaluating Collective Impact Supplement: Sample Questions, Outcomes, and Indicators* (Boston: FSG, 2014), about, https://www.collectiveimpactforum.org/sites/default/files/Guide%20to%20Evaluating%20CI%2003.pdf.

[234] Ferber and White, "Making Public Policy Collective Impact Friendly," 23.

[235] Ferber and White, 23.

[236] Ferber and White, 23.

Table 3. Public Policies that Encourage Collective Impact.[237]

Public Policies That Encourage Collective Impact

CONDITION OF COLLECTIVE IMPACT	PUBLIC POLICIES THAT ALLOW OR INCENTIVIZE EACH CONDITION
Common Agenda	■ Planning grants in addition to implementation grants ■ Requirements to engage partners from multiple sectors
Shared Measurement	■ Data sharing agreements ■ Accountability for shared outcomes
Mutually Reinforcing Activities	■ Blended funding streams ■ Allowances for tailoring to local conditions
Continuous Communication	■ Requirements for documenting the process of collaboration ■ Allowing for adjustment in plans to support emergence
Backbone Support	■ Funding for backbones ■ Grant criteria that require defined backbone functions

In addition to their findings, Lynn et al.'s research identified a list of best practices that practitioners can incorporate in their initiatives for positive outcomes.[238] The principles focus on stakeholder equity and diversity, improvement, leadership, relationships, and adaptability. The eight principles of practice are:

- Design and implement the initiative with priority on equity
- Include community members in the collaborative
- Recruit and co-create with cross-sector partners
- Use data to continuously learn, adapt, and improve
- Cultivate leaders with unique system leadership skills
- Focus on program and system strategies

[237] Source: Ferber and White, 23.

[238] Lynn et al., *When Collective Impact has an Impact*, 17.

- Build a culture that fosters relationships, trust, and respect, across participants
- Customize for local context[239]

The eight principles of practice in addition to the cultural and policy changes identified by Ferber and White can help practitioners mitigate any challenges they encounter during the collective impact process and drive engagement of stakeholders.

Despite the complexities and potential limitations of the process to create a collective impact initiative, practitioners can leverage the abundance of resources and tools available to create and maintain a successful initiative. This research only highlighted a few of the many resources and tools available for collective impact initiatives. The components of collective impact are designed to address some of the weaknesses identified throughout the literature for deceptive messaging response efforts and highlights what those efforts should look like moving forward for a whole-of-society response. While in theory collective impact seems to serve the recommendations from experts identified earlier, the following section assesses if the collective impact method is suitable for the U.S. government to use for building a coordinated response to combat deceptive messaging.

B. ASSESSMENT FOR APPLICABILITY

To determine first if collective impact is appropriate for the U.S. government to adopt, practitioners can start an assessment by using the *Collective Impact Feasibility Framework.* The framework was first presented by FSG, a consulting firm that uses its expertise to help clients around the world create social impact.[240] The framework is a guide that consists of four yes or no questions to discuss about a chosen social problem, such as

---

[239] Lynn et al., 17.

[240] FSG, *Collective Impact Feasibility Framework* (Boston: FSG, 2015), 2, https://www.collectiveimpactforum.org/sites/default/files/Collective%20Impact%20Feasibility%20Framework.pdf; Admas Kanyagia, "Is Collective Impact the Right Approach?," *Collective Impact Forum* (blog), September 15, 2015, https://www.collectiveimpactforum.org/blogs/1051/collective-impact-right-approach.

deceptive messaging.[241] Based on each answer, it signals if collective impact is an appropriate fit for the identified problem and also offers several considerations for the user, even if the answer is no.[242] Admas Kanyagia recommends that a diverse group of stakeholders should "use data, stakeholder perspectives, system maps, and other tools to help local stakeholders assess each question" and "communicate the results of your assessment to the wider community when possible to rally support for future initiatives."[243] The feasibility framework facilitates the necessary conversation across stakeholders to determine enough interest and support for a joint effort to address the identified issue.

The stakeholders that have a role in responding to deceptive messaging, such as U.S. government agencies, private sector companies, civil-society, and academia, are best suited to answer the questions presented in the feasibility framework together. However, based on this research, question two, "are there multiple actors in the system who can influence this social problem?" and the questions under number three, "is the system fragmented, disconnected, and broken?,, "If yes, do multiple sectors need to work together to address the issue?," and "Are the majority of people in the system affected by this social problem?" all seem to signal that collective impact is an appropriate method to pursue for a coordinated response to deceptive messaging. The full framework is illustrated in Figure 3.

---

[241] FSG, 2.

[242] FSG, 2–3.

[243] Kanyagia, "Is Collective Impact the Right Approach?"

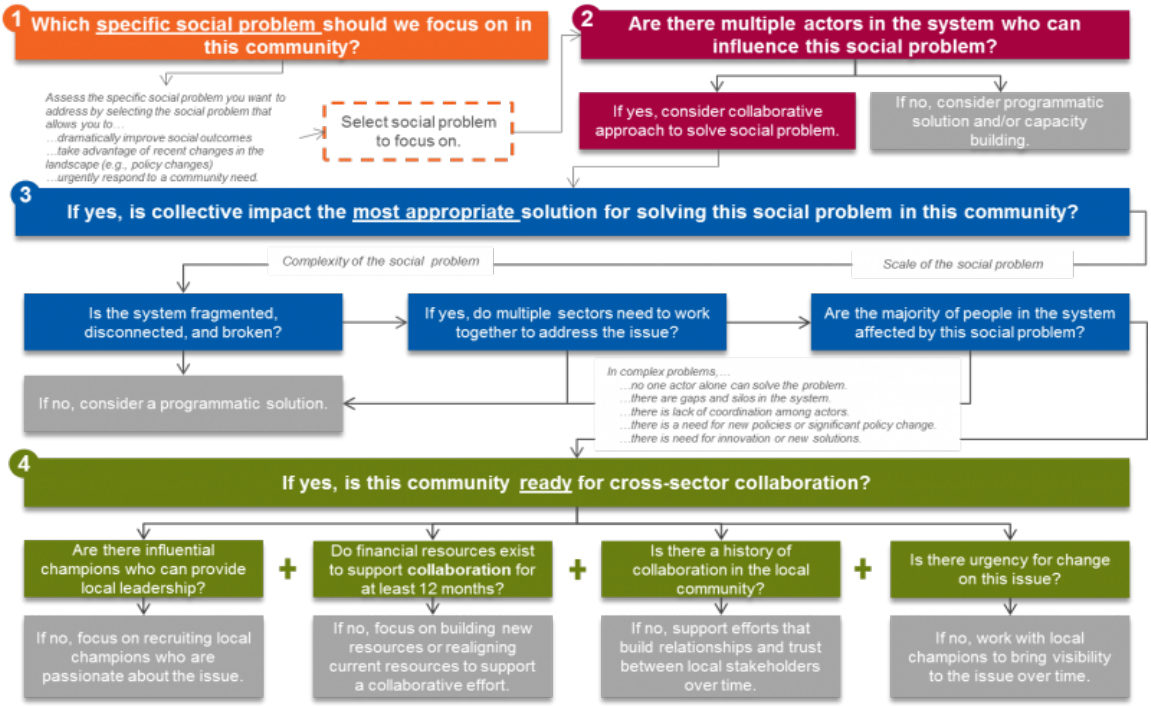

Figure 3. Collective Impact Feasibility Framework.[244]

In addition to the *Collective Impact Feasibility Framework*, it is also worthwhile to examine collective impact use cases. The NYS Juvenile Justice System's effort to reform its operations is one example of a successful initiative.[245] The system had a number of identified inefficiencies, it was labeled as ineffective, and it was deemed to be unsafe.[246] Most notably, "over 60% of youth were rearrested within two years of release" and "state facilities were under investigation by the U.S. Department of Justice for brutal conditions of confinement."[247] These issues presented an urgent demand for broad social change. The NYS Juvenile Justice System is complex and consists of "public and private agencies, nonprofit organizations, and courts, with unique policies and procedures at both the state

---

[244] Source: FSG, *Collective Impact Feasibility Framework*, 3.

[245] New York State Juvenile Justice Advisory Group, *New York State Juvenile Justice*, 1.

[246] New York State Juvenile Justice Advisory Group, 1.

[247] New York State Juvenile Justice Advisory Group, 1.

and local levels" that also connect with other education and mental health systems.[248] Due to the wide variety of stakeholders involved in the system and the need for drastic improvements, stakeholder leaders agreed that collective action was necessary for the needed reforms and collective impact provided a potential framework to drive that change.[249]

The initiative started with a strategic plan, *Safe Communities, Successful Youth: A Shared Vision for the New York State Juvenile Justice System* that set a common ground for the stakeholders that comprise the system.[250] The plan consisted of the following components:

- **Steering committee:** A group composed of key leaders from the many entities across the state that comprise the justice system.
- **Shared vision:** The agreed upon vision statement was, "Across New York State, the juvenile justice system promotes youth success and ensures public safety."[251]
- **Two work groups:** The groups were tasked to identify existing services for youth and examine current data.
- **Action steps:** The actions steps consisted of 10 critical steps organized in three themes: "(1) assuring quality system governance, accountability, and coordination, (2) implementing an effective continuum of services based on best practices, and (3) collecting and sharing data to make information-driven decisions and policy."[252]

---

[248] New York State Juvenile Justice Advisory Group, 1.

[249] New York State Juvenile Justice Advisory Group, 1.

[250] New York State Juvenile Justice Advisory Group, 2.

[251] New York State Juvenile Justice Advisory Group, 2.

[252] New York State Juvenile Justice Advisory Group, 2.

- **Strategic planning action committee (SPAC):** This committee consisted of "leaders from various agencies, organizations, and courts from across the state," to ensure effective implementation of the strategic plan.
- **Backbone staff:** State-provided staff to support the committee funded by three different state agencies.[253]

Two years after the SPAC first met, it reported, "nearly all of the 10 critical near-term action steps had been accomplished or were in progress, ensuring significant gains in governance, accountability, and coordination."[254] An evaluation of the initiative showed measurable success in several parts of the system. Two of the most significant outcomes were that juvenile arrests dropped by nearly a quarter within three years, and approximately half as many youths were in state custody.[255] Stakeholders and evaluators highlighted the accomplishments made across the system in addition to other ancillary benefits:

- New and stronger relationships across the system
- Deeper knowledge of programs and services
- Significant policy changes
- Commitment to data-driven decision-making
- Engagement of local communities
- Empowerment of new stakeholders
- Exponential leverage of the original investment[256]

---

[253] New York State Juvenile Justice Advisory Group, 2.

[254] New York State Juvenile Justice Advisory Group, 3.

[255] New York State Juvenile Justice Advisory Group, 1.

[256] New York State Juvenile Justice Advisory Group, 3–4.

Similar to the Strive initiative, the NYS Juvenile Justice System had an initial investment of just $140,000, but found that the combined resources of engaged stakeholders presented them with resources six times greater than the initial investment. Without the resources of many, the impact of change would likely be less significant. Although the NYS Juvenile Justice System saw measurable success following the implementation of the initiative, it should be noted that causal evidence showing that the results were a direct outcome of collective impact is not immediately available.

Despite the lack of causal evidence in the NYS Juvenile Justice System case, research has been done on other cases to support the effectiveness of collective impact initiatives. Not all collective impact initiatives appear to be as successful as that of the NYS Juvenile Justice System. A study of 25 other initiatives revealed that five of them "did not have documented, meaningful population changes."[257] Researchers pointed out that these initiatives may have not yet had enough time for population change; however, noted differences between the initiatives were seen with evidence of population change and those without.[258] Some of the identified differences included challenges with the quality of communication efforts, obtaining agreement on a common agenda and work plans, measuring impacts, transition of staff or duties, competing initiatives, resource constraints, and political support.[259] This research indicates that the outcomes of a collective impact initiative likely depend on the quality of implementation, as well as control of external factors.

To envision what the elements of a collective impact initiative may look like for deceptive messaging, it is worthwhile to look at the EU's response to disinformation through the lens of the five conditions of collective impact. Although collective impact was not necessarily the EU's method for building coordination efforts, the discussion of its elements earlier in Chapter III embodies and illustrates some of the conditions of collective impact, including a common agenda and mutually reinforcing activities.

---

[257] Lynn et al., *When Collective Impact Has an Impact*, 81.

[258] Lynn et al., 81–83.

[259] Lynn et al., 81–83.

The European Commission's *Communication on Tackling Online Disinformation: A European Approach* represents the potential for a common agenda because it establishes a shared definition of disinformation and the threat it poses across the EU.[260] Furthermore, it presents a vision of a "well-functioning, free, and pluralistic information ecosystem, based on high professional standards."[261] The commission's *Action Plan against Disinformation* goes a step further in outlining specific action items for member states, EU institutions, and online platforms that contribute to the overarching response.[262] While the EU's shared plan seems like a step in the right direction, it is not clear how much input other stakeholders had in the development of each document, beyond the commission's 28 members representing each EU country. While perhaps not a perfect example, it is a very close representation to what a common agenda may look like for deceptive messaging.

In addition to a common agenda, the Rapid Alert System represents a mutually reinforcing activity. The exchange of information between the 28 designated points of contact through the system can help reduce a duplication of effort and coordinate the activities of the others.[263] For example, one agency may be strong at conducting trend analysis, and the other may be an expert in disinformation detection. Rather than both agencies spreading their capacity to do both trend analysis and disinformation detection, they can coordinate those actions. The coordination of those activities would allow each entity to focus more resources on its set of expertise. Those disparate efforts are equally important to the disinformation response and can be bridged in the Rapid Alert System. Connecting that information and reducing a duplication of effort could lead to additional insights for both entities or even support the efforts of another stakeholder in the system. The Rapid Alert System and the framing documents of the EU response to disinformation

---

[260] European Commission, "Tackling Online Disinformation," 3–6.

[261] European Commission, 8.

[262] European Commission, *Joint Communication... Action Plan against Disinformation*, 5–11.

[263] European Union External Action, *Rapid Alert System Strengthening Coordinated and Joint Responses to Disinformation*, 1.

are illustrations of only two conditions of collective impact. An initiative must attain all five conditions to be most effective.

Collective impact initiatives and the supporting resources are specifically designed to address the challenges identified in earlier chapters by establishing a shared definition of the threat and end goal, leadership to organize and align stakeholders and monitor progress, building trust with the private sector, reducing budgetary limitations by pooling resources, and driving equity for mutually beneficial outcomes across stakeholders. Research has shown that initiatives that lacked these qualities did not show meaningful change, and the same results could apply to combating deceptive messaging in the United States should collective impact not be implemented.[264] Based on the alignment with coordination needs, the expected outcome of the feasibility framework, the measurable success in many cases, and noticeable traces of elements in the EU response to disinformation, collective impact is a method that should be strongly considered for adoption among deceptive messaging and information environment stakeholders in the United States.

[264] Lynn et al., *When Collective Impact has an Impact*, 81.

THIS PAGE INTENTIONALLY LEFT BLANK

V. MOBILIZING FOR SYNERGY

A house divided against itself cannot stand.

~Abraham Lincoln[265]

Deceptive messaging poses a significant threat to U.S. society and research suggests that nefarious actors will continue to exploit the information ecosystem and evolve the tactics they use to evade detection and to achieve their geo-political, monetary, or ideological objectives.[266] A meta-analysis of expert recommendations to combat deceptive messaging revealed that the scale and complexity of the threat demands a joint effort across stakeholders in the government, private sector, civil society, academia, and the public to develop a national strategy to combat it. This thesis explored two potential ways the U.S. government could improve coordination efforts to fight deceptive messaging in America using the best practices identified in the EU's response to disinformation and the adoption of the collective impact method. Both approaches can facilitate and accelerate the development of a whole-of-society driven national strategy to fight deceptive messaging in the United States.

A. RECOMMENDATIONS

Deceptive messaging is a global challenge that can manifest into real threats and security challenges for not only elections and government agencies but also for financial sectors, healthcare industries, businesses, organizations, or entire communities. Polyakova and Fried made it clear that, "State-sponsored disinformation campaigns are upping their game, and they won't be limited to election cycles. Democracies are still playing catch-up

---

[265] Abraham Lincoln, excerpt from "Famous Speeches [of] Abraham Lincoln," Digital Public Library of America, c. 1935, http://dp.la/item/1ca86fc8c80f378ffd703603369523aa.

[266] S. *Foreign Influence Operations and their Use of Social Media Platforms*, 1–6; Ignatidou, *EU–U.S. Cooperation on Tackling Disinformation*, 5.

—the United States barely so."[267] The U.S. government must get serious about building coordination that extends beyond ad hoc partnerships and collaborations, with FSLTT agencies, the private sector, media companies, academia, civil society, international allies, and the public to build an effective national strategy to combat deceptive messaging.

Malicious actors spreading deceptive messaging campaigns use the divisiveness of U.S. society to their advantage.[268] Coordination should be made a priority, and seen as the first step toward a national strategy to ensure input from stakeholders with the knowledge, expertise, access to information, and skill sets needed to build an effective response. The conversations in this research about which multi-stakeholder model the U.S. government should adopt or the free flow of information between government and non-government stakeholders carries little weight without first establishing relationships, trust, buy-in, clear rules of engagement, equity in communication, mutually beneficial solutions, and a collective conversation with stakeholders to determine the best path forward for everyone.

Collective impact is just one method that government practitioners can use to achieve the relationship and trust building process. The five conditions and the five phases of impact provide specific action items and a plan that focuses on dialogue, outreach, and building synergy around a common goal and operating picture.[269] Collective impact is a well-studied model that has proven to make "meaningful changes" in response to complex social problems, such as the outcomes observed in the NYS Juvenile Justice System initiative.[270] By strategically aligning stakeholders around a common goal and operating picture, the U.S. government can overcome government budget limitations by compounding available resources and manpower to mount a response more equal in size to the threat, as seen with the Strive initiative.[271] The success of collective impact and

---

[267] Polyakova and Fried, "Europe Is Starting to Tackle Disinformation."

[268] S., *United States Senate Foreign Relations Subcommittee on State Department and USAID Management, International Operations, and Bilateral International Development Hearing*, 2.

[269] Kania and Kramer, "Collective Impact," 39–41; Tamarack Institute, *Collective Impact Self-Assessment and Planning Tool*, 1–3.

[270] Stachowiak and Gase, "Does Collective Impact Really Make an Impact?"; New York State Juvenile Justice Advisory Group, *New York State Juvenile Justice*, 1–2.

[271] Kania and Kramer, "Collective Impact," 41.

resources that provide a roadmap forward make it a valuable option to tackle the whole-of-society coordination challenge to combat deceptive messaging in U.S. society.

The U.S. government should also use collective impact as a plan to help overcome stakeholder participation challenges with private-sector companies, as identified by scholars and experienced by the EU.[272] A precedent has been established for private sector companies to voluntarily share data with government agencies for other public safety initiatives. For example, when Google identifies a "threat to life or serious bodily harm" on its platforms, it reports the information to the Northern California Regional Intelligence Center to ensure that any necessary law enforcement intervention occurs.[273] However, speaking as a participant, this process was the outcome of several months of dialogue and in-person conversations of personnel to build relationships and understand the perspectives and boundaries within which each party was operating. A voluntary agreement or U.S. code of practice, similar to the EU code, may be a good place to start to establish rules of engagement and document the needs, capabilities, and plans for stakeholders to contribute to a response.

Developing any coordination or stakeholder relationship will be challenging without a person or entity driving and organizing those efforts. Congress should immediately identify and clarify which agency or entity will be mandated to lead deceptive messaging strategy and coordination development. With adequate funding, support, mandates, and messaging, the DHS may be a logical option to lead this endeavor since it has been mounting a foreign influence response with election security efforts and the CFITF. Furthermore, the Countering Foreign Influence Subcommittee tasked the DHS in 2019 to become the leading entity to establish a national strategy to counter foreign

---

[272] Busch and Givens, "Public-Private Partnerships in Homeland Security, 10–15; Bodine-Baron et al., *Countering Russian Social Media Influence*, 44; European Commission, "Code of Practice against Disinformation," last modified January 29, 2019, https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en; European Commission, *Joint Communication...Report on the Implementation of the Action Plan against Disinformation*.

[273] *Written Testimony of Derek Slater Director, Information Policy, Google LLC United States Senate Committee on Commerce, Science, and Transportation "Mass Violence, Extremism, and Digital Responsibility,"* Senate, 116th Cong., 1st sess., September 18, 2019, 2–3, https://www.commerce.senate.gov/services/files/B74BE056-4446-470B-8B3C-F2E4463AFB66.

influence and ensure effective coordination.[274] Other benefits to considering the DHS for this role are apparent since it is well connected to and possesses existing practices, systems, and knowledge that may be leveraged and repurposed for combatting deceptive messaging in America. Two examples include the National Network of Fusion Centers and the Homeland Security Information Network (HSIN).

From my professional experience, fusion centers have been developing and refining information sharing and reporting networks since 2001 that connect FSLTT law enforcement, the intelligence community, public safety agencies, the public, faith-based communities, medical communities, and in many cases, the private sector. The established network can be a force multiplier to detect and report malicious deceptive messaging campaigns for tactical response or strategic reporting. Fusion centers' daily operations and grant requirements rely heavily on using HSIN to communicate with partners and across the network.[275]

The DHS created HSIN, a secure digital platform, to reduce a duplication of effort and facilitate information sharing and collaboration across the nation's vast intelligence network.[276] The system consists of over 110,000 tribal, territorial, state, local, federal, non-profit, private sector, and international vetted users that can post projects for collaboration and share sensitive, unclassified information to thousands of other intelligence stakeholders in real-time.[277] HSIN is similar to the Rapid Alert System in the EU's response to disinformation, which successfully increased the interactions, trust, and communication between EU stakeholders.[278] U.S. stakeholders can use the fusion center

---

[274] Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*, 10.

[275] Department of Homeland Security, *2018 National Network of Fusion Centers Final Report* (Washington, DC: Department of Homeland Security, 2018), B–1, https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

[276] Homeland Security Information Network, *Homeland Security Information Network (HSIN) FY 2018 Annual Report* (Washington, DC: Department of Homeland Security, 2019), 1–30, https://www.dhs.gov/sites/default/files/publications/hsin-fy2018-annual-report.pdf.

[277] Homeland Security Information Network, 4.

[278] European Commission, *Joint Communication ...Report on the Implementation of the Action Plan against Disinformation*; European Union External Action, *Rapid Alert System Strengthening Coordinated and Joint Responses to Disinformation*, 1.

network and HSIN to detect and share information about deceptive messaging campaigns and tactics in real-time, while improving relationships and coordination simultaneously.

U.S. government practitioners should also leverage the many other best practices identified in the EU response to disinformation, such as creating a joint action plan or common agenda, providing support from the top tiers of the U.S. administration and government, setting hard deadlines for report publications, and making information available and accessible to the public and stakeholders. Practitioners, however, should not stop at identifying best practices from the EU and also seek more from other stakeholders, such as civil society disinformation tracking efforts, and other countries, such as Finland, which is held in high regard for its resilience to deceptive messaging campaigns and media literacy programs.[279]

Developing a common agenda is the first condition of the collective impact process and the European Commission's *Communication on Tackling Online Disinformation: A European Approach* and the *Action Plan against Disinformation* provide concrete examples of what one can look like for a response to disinformation.[280] The development of these two documents may have been challenging had it not been for the support of the top levels of EU governance. Support from the presidential administration and Congress will be helpful to address budget challenges, and enforce binding agreements or legislation and the publication of necessary reports.

The availability and accessibility of information is critical for building public resilience, and the continuous use of deadlines throughout the EU response to disinformation established a degree of accountability and expectations that can be helpful to prevent the stagnation of progress. Whether or not deadlines directly contributed to the EU's progress, its response has matured and grown much quicker than that of the United States.[281] In addition to ensuring the availability of updated information, other government

---

[279] Polyakova and Fried, *Democratic Defense against Disinformation 2.0*, 3; De Jong et al., *Inside the Kremlin House of Mirrors*, 25–34.

[280] European Commission, *Communication from the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*; European Commission, *Joint Communication... Action Plan against Disinformation*.

[281] Polyakova and Fried, "Europe Is Starting to Tackle Disinformation."

stakeholders producing products and reports should follow the example set by the DHS CISA product, *The War on Pineapple*, because it is easy to find, consume, and recall. To expand on consumption principles, products should not only be concise and written in plain language, but they must also be published in more languages, than just English, to reach all demographics and communities within U.S. society.

Awareness campaigns can also be used to help develop training and awareness efforts for government personnel and journalists. Although training resources are at a nascent stage, materials are available online to facilitate the development of a program. For example, RAND sponsors a webpage called "Tools That Fight Disinformation Online" that is a robust library of resources for education, training, detection, tracking, verification, and more.[282] The trust in government and media is fragile, and personnel in those professions must set an example for resilience to disinformation to ensure the public is provided with true and accurate narratives to form their own opinions or beliefs.

Training for personnel and stakeholders should also consist of building awareness about response efforts in the United States. As identified in this research, many government agencies, beyond the DHS and GEC, have ramped up efforts against foreign influence, disinformation, and information warfare. Having access to information about which stakeholders are performing certain actions will be critical to facilitate in the beginning phases of a collective impact initiative to truly align stakeholders, and this resource does not seem to currently exist. Table 4 compiles the government agencies that have been identified via open source as contributing some variation of effort to fight deceptive messaging. Due to a lack of time and resources, research on specific agencies was limited to only government stakeholders. However, it can and should be used as a starting place for others to expand and include other information, such as the role and focus of each agency to help other stakeholders prioritize objectives and align them with the broader collective. Table 4 is still being updated and thus is not final. U.S. government practitioners should pursue the expansion of this resource and make it, or parts of it, widely available to non-government agencies or even the public to increase transparency and trust.

---

[282] "Tools that Fight Disinformation Online," RAND, accessed August 28, 2020, https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html.

Table 4. U.S. Government Agencies Fighting Deceptive Messaging.

Department of Homeland Security (DHS)[283]	Department of Defense (DOD-EUCOM, USCYBERCOM, SOCOM, DARPA)[284]
Office of the Director of National Intelligence (ODNI)[285]	National Counterintelligence and Security Center (NCSC)[286]
U.S. Department of Justice (USDOJ)[287]	Department of Treasury (DOT)[288]
Global Engagement Center (GEC)[289]	National Security Agency (NSA)[290]
FBI—Foreign Influence Task Force (FITF)[291]	U.S. Agency for Global Media (USAGM)[292]
Russia Influence Group (RIG) (Co-chaired by DOS and DOD)[293]	United States Agency for International Development (USAID)[294]

[283] "Election Security," Department of Homeland Security, last modified March 5, 2019, https://www.dhs.gov/topic/election-security.

[284] Polyakova and Fried, *Democratic Defense against Disinformation 2.0*; Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 32.

[285] Jonathan Andrews, "Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," Office of the Director of National Intelligence, October 19, 2018,.

[286] *Statement of Lea Gabrielle Special Envoy & Coordinator for the Global Engagement Center, U.S. Department of State before the House Appropriations Subcommittee on State, Foreign Operations, and Related Programs "United States Efforts to Counter Russian Disinformation and Malign Influence,"* House of Representatives, 116th Cong., 1st sess., July 10, 2019, 3.

[287] Andrews, "Joint Statement from the ODNI, DOJ, FBI and DHS."

[288] Polyakova and Fried, *Democratic Defense against Disinformation 2.0*.

[289] Department of State, "Global Engagement Center."

[290] S., *United States Senate Foreign Relations Subcommittee on State Department and USAID Management, International Operations, and Bilateral International Development Hearing*, 6.

[291] Federal Bureau of Investigation, "Combating Foreign Influence," What We Investigate, accessed March 3, 2019, https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

[292] *Statement of John Lansing CEO and Director U.S. Agency for Global Media before the House Appropriations Subcommittee on State, Foreign Operations, and Related Programs "United States Efforts to Counter Russian Disinformation and Malign Influence,"* House of Representatives, 116th Cong., 1st sess., July 10, 2019, 1–8.

[293] H.R., *Statement of Lea Gabrielle Special Envoy & Coordinator for the Global Engagement Center*, 2.

[294] Brock Bierman, "Remarks by Assistant Administrator Brock Bierman, The McCain Institute Tbilisi Conference: Discussion on Disinformation," USAID, September 9, 2019.

B. CONCLUSIONS

This thesis aimed to progress the U.S. government's response to deceptive messaging by identifying and simplifying policy prescriptions, determining which prescriptions should be a priority for a national strategy, and presenting methods and resources available to accomplish those priorities. Deceptive messaging is not a threat that can be eliminated, and it may take several years of committed effort before any measurable or meaningful results are observed. However, it is critical to look at the recommendations for a response in smaller units that can be prioritized and translated into specific action items that over time will contribute to long-term societal resilience.

Deceptive messaging campaigns are only expected to become more pervasive and more difficult to detect, track, and attribute with the adversary adapting to countermeasures and policies, and the evolution of technology, such as deepfakes and encryption. In fact, other countries are experiencing the spread of disinformation through private platforms and closed groups or instant messengers, and the abilities of AI to generate counterfeit media are expected to surpass those of AI to identify such media by 2020.[295] The lack of visibility or inability to identify deceptive messaging will make information sharing, collaboration, and public engagement even more important.

Grave consequences may result if deceptive messaging response efforts remain independent or a loose patchwork. In fact, the siloed nature of the intelligence community was cited by the 9/11 Commission as a weakness leading up to the terrorist attacks.[296] The United States should capitalize on the lessons learned about the value of joint action from *The 9/11 Commission Report* to strengthen its defenses against deceptive messaging before the next major attack. Once a deceptive messaging campaign has taken root in society, effectively counteracting that message or reversing its effects is advantageous. The U.S. government should be more proactive in creating a unified national strategy that starts with

---

[295] H.R., *Statement of Nina Jankowicz Woodrow Wilson International Center for Scholars*; Gartner IT Glossary, "Virtual Assistant (VA)," Gartner, accessed October 15, 2018, https://www.gartner.com/it-glossary/virtual-assistant-va/.

[296] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 416–419.

a collective impact initiative as its foundation and uses best practices from the EU to accelerate those efforts. Should the U.S. government not take the necessary steps to bring together important parts of society to challenge those who wish to harm the U.S. via cyber-based deceptive messaging, it may be on a path in which fake news-induced catastrophes are reality.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. THE WAR ON PINEAPPLE

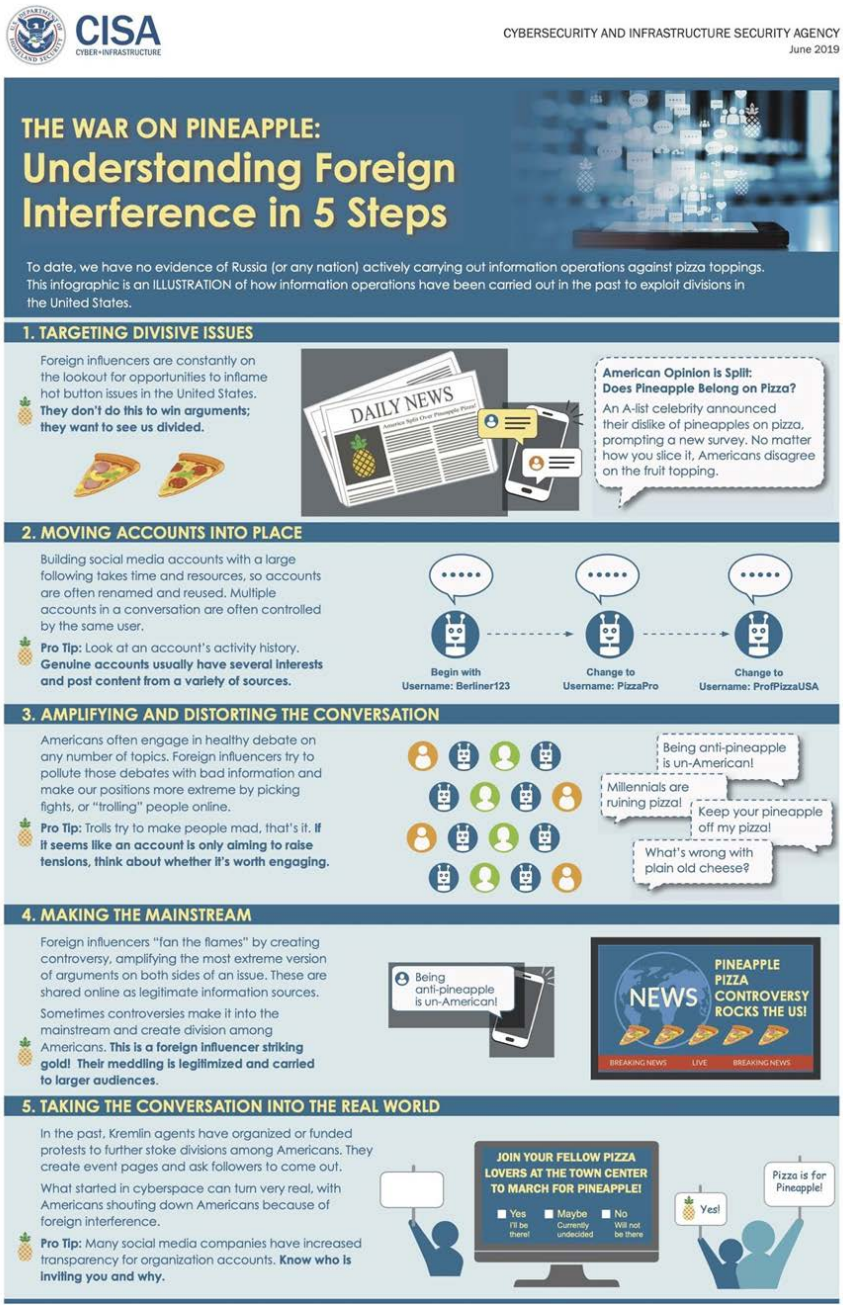

Figure 4. The War on Pineapple and Understanding Foreign Interference.[297]

[297] Source: Cybersecurity and Infrastructure Security Agency, *The War on Pineapple*, 1.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. GLOSSARY OF TERMS

Cognitive Security: Focus on protection from the exploitation of cognitive biases and social influence of large public groups.[298]

Deceptive Messaging: Comprehensive term that includes information defined as fake news, propaganda, disinformation, misinformation, and mal-information, communicated or shared intentionally or unintentionally to mislead the consumer.

Deepfake: "An audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual."[299]

Disinformation: "All forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit."[300]

Fake News: "Hoax-based stories that perpetuate hearsay, rumors, and misinformation."[301]

Foreign Influence: "Malign actions taken by foreign governments or foreign actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies."[302]

---

[298] Waltzman, *The Weaponization of Information*, 4–5.

[299] Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Cong., 2nd sess. (2018), 2, https://www.congress.gov/115/bills/s3805/BILLS-115s3805is.pdf.

[300] Bayer et al., *Disinformation and Propaganda*, 25.

[301] Paul Mihailidis and Samantha Viotty, "Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in 'Post-Fact' Society," *American Behavioral Scientist* 61, no. 4 (2017): 441–454, https://doi.org/10.1177/0002764217701217.

[302] Homeland Security Advisory Council, Countering Foreign Influence Subcommittee, *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*, 11.

Hybrid Threats: Threats that "combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives."[303]

Information Environment: "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[304]

Information Laundering: "The process through which the 'internet's unique properties allow subversive social movements to not only grow globally, but also to quietly legitimize their causes through a borrowed network of associations.'"[305]

Mal-Information: "When genuine information is shared to cause harm."[306]

Media Literacy: "The ability to access, analyze, evaluate, and communicate messages in a wide variety of forms."[307]

Misinformation: "False or misleading information, whether or not the agent spreading the information intends to mislead"[308]

Propaganda: "The deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist."[309]

---

[303] European Union, *A Europe that Protects: Countering Hybrid Threats* (Brussels: European Union, 2018), 1, https://eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf.

[304] Department of Defense, *Department of Defense Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, 2016), 3, https://dod.defense.gov/Portals/1/Documents/pubs/DOD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

[305] Korta, "Fake News, Conspiracy Theories, and Lies," 1–10.

[306] Bayer et al., *Disinformation and Propaganda*, 26.

[307] Huguet et al., *Exploring Media Literacy Education*, 45.

[308] Giorgi Revishvili, "Two Sides of the Same Coin: Misinformation and Disinformation," Sunlight Foundation, May 23, 2019, https://sunlightfoundation.com/2019/05/23/two-sides-of-the-same-coin-misinformation-and-disinformation/.

[309] Garth S. Jowett and Victoria J. O'Donnell, *Propaganda & Persuasion*, 6th ed. (Thousand Oaks, CA: SAGE, 2014), 7.

Whole-of-Society Approach: A joint and coordinated effort across a group of diverse stakeholders that includes, but may not be limited to, federal, state, and local government, the private sector, civil society and non-governmental organizations, academia, the public, and international allies.[310]

[310] Fly, Rosenberger, and Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, 17–22; Warner, "A New Doctrine for Cyberwarfare & Information Operations."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agarwal, Shruti, Hany Farid, Yuming Gu, Mingming He, Koki Nagano, and Hao Li. "Protecting World Leaders Against Deep Fakes." In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops* (June 2019): 38–45. https://farid.berkeley.edu/downloads/publications/cvpr19/cvpr19a.pdf.

Alexander, Sam, Peter M., Adam Cambridge, S. Renee Farner, Robert Kang, Stephanie Kiefer, and Kawika Tatayama et al. *Combatting Targeted Disinformation Campaigns: A Whole-of-Society-Issue*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

Alliance for Securing Democracy. "Hamilton 2.0 Dashboard." Accessed September 7, 2019. https://securingdemocracy.gmfus.org/hamilton-dashboard/.

Andrews, Jonathan. "Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections." Office of the Director of National Intelligence, October 19, 2018. https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections.

Andrews, Thomas. "Soviet Subversion of the Free World Press." April 24, 2011. YouTube. Video, 1:21:28. https://www.youtube.com/watch?v=Cnf0I2dQ0i0.

Barrett, Paul. *Tackling Domestic Disinformation: What the Social Media Companies Need to Do*. New York City: NYU Stern, 2019. https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_domestic_disinformation_digital?e=31640827/68184927.

Bayer, Judit, Natalija Bitiukova, Petra Bárd, 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*. Brussels: European Union, Policy Department for Citizens' Rights and Constitutional Affairs, 2019. http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

Bierman, Brock. "Remarks by Assistant Administrator Brock Bierman, The McCain Institute Tbilisi Conference: Discussion on Disinformation." USAID, September 9, 2019. https://www.usaid.gov/news-information/speeches/remarks-assistant-administrator-brock-bierman-mccain-institute-tbilisi.

Blackwill, Robert D., and Philip H. Gordon. *Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*. Washington, DC: Council on Foreign Relations, 2018. https://www.cfr.org/report/containing-russia.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger. *Countering Russian Social Media Influence*. Santa Monica, CA: RAND, 2018. https://doi.org/10.7249/RR2740.

Bradshaw, Samantha, and Philip N. Howard. *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Oxford, UK: Oxford Internet Institute's Computational Propaganda Research Project, 2018. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

Busch, Nathan E., and Austen D. Givens. "Public-Private Partnerships in Homeland Security: Opportunities and Challenges." *Homeland Security Affairs* 8, art. 8 (October 2012). https://www.hsaj.org/articles/233.

Canadian Security Intelligence Service. *Who Said What?: The Security Challenges of Modern Disinformation*. Ottawa, ON: Canadian Security Intelligence Service, 2018. https://www.canada.ca/en/security-intelligence-service/corporate/publications/who-said-what-the-security-challenges-of-modern-disinformation.html.

Canan, Mustafa, and Rik Warren. "Cognitive Schemas and Disinformation Effects on Decision Making in Lay Populations." Paper presented at the 13th International Conference on Cyber Warfare and Security (ICCWS 2018). Washington, DC, March 24, 2018. https://www.researchgate.net/publication/327845605_Cognitive_Schemas_and_Disinformation_Effects_on_Decision_Making_in_Lay_Populations.

Chaffee, Ian. "Who's to Blame for Fake News and What Can Be Done about It?." USC News, December 15, 2016. https://news.usc.edu/113738/whos-to-blame-for-fake-news-and-what-can-be-done-about-it/.

Charlton, Emma. "How Finland is Fighting Fake News—in the Classroom." World Economic Forum, May 21, 2019. https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/.

Claesson, Annina. "Coming Together to Fight Fake News: Lessons from the European Approach to Disinformation." *New Perspectives in Foreign Policy*, no. 17 (Spring 2019): 13–19. https://www.csis.org/coming-together-fight-fake-news-lessons-european-approach-disinformation.

Coats, Daniel. *2018 Worldwide Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2018. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

———. *2019 Worldwide Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

———. *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community.* Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Council of the European Union. *Outcome of the Council Meeting, 3613rd Council Meeting, Foreign Affairs, Luxembourg, 16April2018*. Brussels: Press, 2018. https://www.consilium.europa.eu/media/33743/st07997-en18.pdf.

Cybersecurity and Infrastructure Security Agency. *#Protect2020 Strategic Plan*. Washington, DC: Department of Homeland Security, 2020. https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan_FINAL%202.7.20%20508.pdf.

———. *The War on Pineapple: Understanding Foreign Interference in 5 Steps*. Rosslyn, Arlington, VA: Cybersecurity and Infrastructure Security Agency, 2019. https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf.

De Jong, Sijbren, Tim Sweijs, Katarina Kertysova, and Roel Bos. *Inside the Kremlin House of Mirrors: How Liberal Democracies Can Counter Russian Disinformation and Societal Interference*. The Hague, Netherlands: The Hague Centre for Strategic Studies, 2017. https://hcss.nl/report/inside-kremlin-house-mirrors-how-liberal-democracies-can-counter-russian-disinformation-0.

Deeks, Ashley, Sabrina McCubbin, and Cody M. Poplin. "Addressing Russian Influence: What Can We Learn from U.S. Cold War Counter-Propaganda Efforts?" *Lawfare*, October 25, 2017. https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts.

Department of Defense. *Department of Defense Strategy for Operations in the Information Environment*. Washington, DC: Department of Defense, 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DOD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

Department of Homeland Security. *2018 National Network of Fusion Centers Final Report*. Washington, DC: Department of Homeland Security, 2018. https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

———. “Election Security.” Last modified March 5, 2019. https://www.dhs.gov/topic/election-security.

Department of Homeland Security Cybersecurity and Infrastructure Security Agency. “Foreign Interference.” Last revised December 2, 2019. https://www.cisa.gov/publication/foreign-interference.

Department of State. “About Us—Global Engagement Center.” Accessed September 6, 2019. https://www.state.gov/about-us-global-engagement-center/.

———. “Global Engagement Center.” Accessed February 8, 2019. https://www.state.gov/r/gec/.

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*. Scottsdale, AZ: New Foundation Organization, 2018. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf.

Donald, Brooke. “Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online.” Stanford Graduate School of Education, November 22, 2016. https://ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility-information-online.

EdVenture Partners. “About.” Accessed July 17, 2020. https://www.edventurepartners.com/about.

———. “Our Work.” Accessed September 2, 2019. https://www.edventurepartners.com/our-work.

EEAS Strategic Communications and Information Analysis Division. “EEAS Special Report: Disinformation on the Coronavirus—Short Assessment of the Information Environment.” March 19, 2020. https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/.

European Commission. *Action Plan against Disinformation: Report on Progress*. Brussels: European Commission, 2019. https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf.

———. “C(2019) 58 Final.” Official memorandum. Brussels: European Commission, 2019. https://ec.europa.eu/dgs/secretariat_general/relations/relations_other/npo/docs/netherlands/2018/com20180236/com20180236_eerstekamer_reply_en.pdf.

———. “Code of Practice against Disinformation.” Last modified January 29, 2019. https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en.

———. “Code of Practice on Disinformation.” Digital Single Market, September 26, 2018. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

———. *Communication from the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling Online Disinformation: A European Approach*. Brussels: European Commission, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN.

———. *EU Code of Practice on Disinformation*. Brussels: European Commission, 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

———. *European Commission Contribution to the European Council: Action Plan against Disinformation*. Brussels: European Commission, 2018. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

———. *Fact Sheet—Questions and Answers—The EU Steps Up Action against Disinformation*. Brussels: European Commission, 2018. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_18_6648/MEMO_18_6648_EN.pdf.

———. “Joint Communication to the European Parliament and the Council Joint Framework on Countering Hybrid Threats a European Union Response.” European Commission, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

———. *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats.* Brussels: European Commission, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en.

———. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the Implementation of the Action Plan against Disinformation*. Brussels: European Commission, 2019. https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

———. *Report from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the Implementation of the Communication: "Tacking Online Disinformation: A European Approach."* Brussels: European Commission, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0794&from=EN.

———. "Tackling Online Disinformation." Last modified June 17, 2019. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation.

European External Action Service, European Commission. "Questions and Answers about the East StratCom Task Force." May 12, 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

European Union. *A Europe that Protects: Countering Hybrid Threats*. Brussels: European Union, 2018. https://eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf.

European Union External Action. *Rapid Alert System Strengthening Coordinated and Joint Responses to Disinformation*. Brussels: European Union External Action, 2019. https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.

Farwell, James P. "Countering Russian Meddling in U.S. Political Processes." *Parameters* 48, no. 1 (Spring 2018): 37–47. https://www.socom.mil/SovereignChallenge/Sovereign%20Challenge%20Publications/Countering%20Russian%20Meddling%20in%20US%20Political%20Processes.pdf.

Federal Bureau of Investigation. "Combating Foreign Influence." What We Investigate. Accessed March 3, 2019, https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

Ferber, Thaddeus, and Erin White. "Making Public Policy Collective Impact Friendly." *Stanford Innovation Review* 12, no. 4 (Fall 2014): 22–23. https://ssir.org/pdf/Fall_2014_Making_Public_Policy_Collective_Impact_Friendly.pdf.

FireEye. *Suspected Iranian Influence Operation: Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences*. Milpitas, CA: FireEye, 2018. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf.

Fly, Jamie, Laura Rosenberger, and David Salvo. *Policy Blueprint for Countering Authoritarian Interference in Democracies*. Washington, DC: The German Marshall Fund of the United States, 2018. http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

Fried, Daniel, and Alina Polyakova. *Democratic Defense against Disinformation*. Washington, DC: Atlantic Council, 2018. https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf.

FSG. *Collective Impact Feasibility Framework*. Boston: FSG, 2015. https://www.collectiveimpactforum.org/sites/default/files/Collective%20Impact%20Feasibility%20Framework.pdf.

Gartner IT Glossary. "Virtual Assistant (VA)." Gartner. Accessed October 15, 2018. https://www.gartner.com/it-glossary/virtual-assistant-va/.

General Secretariat of the Council. *European Council Meeting (19 and 20 March 2015)–Conclusions*. EUCO 11/15. Brussels: European Council, 2015. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.

Ghosh, Dipayan, and Ben Scott. *#DigitalDeceit: The Technologies behind Precision Propaganda on the Internet*. Washington, DC: New America, 2018. https://d1y8sb8igg2f8e.cloudfront.net/documents/digital-deceit-final-v3.pdf.

Goldman, Russell. "Reading Fake News, Pakistani Minister Directs Nuclear Threat at Israel." *New York Times*, December 24, 2016. https://www.nytimes.com/2016/12/24/world/asia/pakistan-israel-khawaja-asif-fake-news-nuclear.html.

Hanlon, Bradley. *A Long Way to Go: Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*. No. 041. Washington, DC: German Marshall Fund, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/12/A-Long-Way-to-Go-Analyzing-Facebook-Twitter-and-Googles-Efforts-to-Combat-Foreign-Interference.pdf.

Harari, Yuval. *21 Lessons for the 21st Century*. New York: Penguin Random House LLC, 2018.

Harder, Henry. "Explanatory Case Study." In *Encyclopedia of Case Study Research*, edited by Albert Mills, Gabrielle Durepos and Elden Wiebe, 371–375. Thousand Oaks: SAGE Publications Inc., 2012. https://dx.doi.org/10.4135/9781412957397.

Homeland Security Advisory Council, Countering Foreign Influence Subcommittee. *Homeland Security Advisory Council Countering Interim Report of the Countering Foreign Influence Subcommittee*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/sites/default/files/publications/ope/hsac/19_0521_final-interim-report-of-countering-foreign-influence-subcommittee.pdf.

Homeland Security Information Network. *Homeland Security Information Network (HSIN) FY 2018 Annual Report*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/sites/default/files/publications/HSIN-FY2018-Annual-Report.pdf.

Huguet, Alice, Jennifer Kavanagh, Garrett Baker, and Marjory S. Blumenthal. *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay*. RR-3050-RC. Santa Monica, CA: RAND, 2019. https://www.rand.org/pubs/research_reports/RR3050.html.

Ignatidou, Sophia. *EU–U.S. Cooperation on Tackling Disinformation*. London: Chatham House, 2019. https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf.

Innes, Martin, Helen Innes, Diyana Dobreva, Steven Chermak, Laura Huey, and Alyce McGovern. *From Minutes to Months: A Rapid Assessment of the Impact of Media and Social Media during and after Terror Events*. Cardiff, UK: Cardiff University, Crime & Security Research Institute, 2018. https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bc74f950d929708f7733b3c/1539788716177/M2M+Report+%5BFinal%5D.pdf.

Insikt Group. *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*. Somerville, MA: Recorded Future, 2019. https://www.recordedfuture.com/china-social-media-operations/.

International Telecommunications Union. “Statistics.” Accessed August 6, 2019. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Jowett, Garth S., and Victoria J. O’Donnell. *Propaganda & Persuasion*. 6th ed. Thousand Oaks, CA: SAGE, 2014.

Kania, John, and Mark Kramer. “Collective Impact.” *Stanford Social Innovation Review* 9, no. 1 (Winter 2011): 36–41. https://ssir.org/articles/entry/collective_impact.

Kania, John, Fay Hanleybrown, and Jennifer Splansky Juster. “Essential Mindset Shifts for Collective Impact.” *Stanford Social Innovation Review* 12, no. 4 (Fall 2014): 2–5. https://ssir.org/articles/entry/essential_mindset_shifts_for_collective_impact.

Kanyagia, Admas, "Is Collective Impact the Right Approach?." *Collective Impact Forum* (blog), September 15, 2015. https://www.collectiveimpactforum.org/blogs/1051/collective-impact-right-approach.

Kavanagh, Jennifer, and Michael D. Rich. *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. RR-2314-RC. Santa Monica, CA: RAND, 2018. https://www.rand.org/pubs/research_reports/RR2314.html.

Korta, Samantha M. "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security." Master's thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/58322.

Lessenski, Marin. *Common Sense Wanted Resilience to 'Post-Truth' and its Predictors in the New Media Literacy Index 2018*. Sofia, BG: Open Society Institute–Sofia, 2018. https://osis.bg/wp-content/uploads/2018/04/MediaLiteracyIndex2018_publishENG.pdf.

Lewsey, Fred. "Fake News 'Vaccine' Works: 'Pre-Bunk' Game Reduces Susceptibility to Disinformation." University of Cambridge, June 25, 2019. https://www.cam.ac.uk/research/news/fake-news-vaccine-works-pre-bunk-game-reduces-susceptibility-to-disinformation.

Lincoln. Abraham. Excerpt from "Famous Speeches [of] Abraham Lincoln." Digital Public Library of America, c. 1935. http://dp.la/item/1ca86fc8c80f378ffd703603369523aa.

Lu, Michelle. *Collective Impact in Promise Zones*. Philadelphia: Wharton, University of Pennsylvania, 2018. https://publicpolicy.wharton.upenn.edu/live/news/2674-collective-impact-in-promise-zones.

Lynn, Jewlya, Lauren Gase, Julia Roos, Sophie Oppenheimer, Alex Dane, Sarah Stachowiak, and Terri Akey et al. *When Collective Impact Has an Impact: A Cross-Site Study of 25 Collective Impact Initiatives*. Seattle, WA: ORS Impact, 2018. https://www.orsimpact.com/DirectoryAttachments/10262018_111513_477_CI_Study_Report_10-26-2018.pdf.

McChrystal, Stanley A., Tantum Collins, David Silverman, and Chris Fussell. *Team of Teams: New Rules of Engagement for a Complex World*. New York: Penguin Publishing Group, 2015. Kindle.

McGeehan, Timothy. "Countering Russian Disinformation." *Parameters* 48, no. 1 (Spring 2018): 54–56. https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf.

Meleshevich, Kirill, and Bret Schafer. *Online Information Laundering: The Role of Social Media*. Washington, DC: Alliance for Securing Democracy, 2018. https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/.

Mihailidis, Paul, and Samantha Viotty. "Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in 'Post-Fact' Society." *American Behavioral Scientist* 61, no. 4 (2017): 441–454. https://doi.org/10.1177/0002764217701217.

Morgan, Jonathon. "Facebook and Google Need to Own their Role in Spreading Misinformation—and Fix It." October 9, 2017. https://www.cnn.com/2017/10/09/opinions/social-media-platforms-spreading-disinformation-opinion-morgan/index.html.

Mueller, Robert S. III. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Department of Justice, 2019. https://www.justice.gov/storage/report.pdf.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton, 2004.

National Counterterrorism Center. "Partnerships." Accessed September 2, 2019. https://www.dni.gov/index.php/nctc-how-we-work/partnerships.

Nemr, Christina, and William Gangware. *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*. Washington, DC: Park Advisors, 2019. https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

New York State Juvenile Justice Advisory Group. *New York State Juvenile Justice: Progress toward System Excellence*. Boston, MA: FGS, 2014. https://www.collectiveimpactforum.org/sites/default/files/NYS_Juvenile_Justice_Progress_Report_0.pdf.

Peterson, Nicole, ed. *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper*. Washington, DC: Department of Defense, Strategic Multilayer Assessment Program, 2019. https://www.politico.com/f/?id=0000016b-a5a1-d241-adff-fdf908e00001.

Nowell, Lorelli S., Jill M. Norris, Deborah E. White, and Nancy J. Moules. "Thematic Analysis: Striving to Meet the Trustworthiness Criteria." *International Journal of Qualitative Methods* 16, no. 1 (2017): 1–13. https://doi.org/10.1177/1609406917733847.

Plasilova, Iva, Jordan Hill, Malin Carlberg, Marion Goubet, and Richard Procee. *Study for the "Assessment of the implementation of the Code of Practice on Disinformation*. Luxembourg: Publications Office of the European Union, 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66649.

Polyakova, Alina, and Daniel Fried. *Democratic Defense against Disinformation 2.0*. Washington, DC: Atlantic Council Eurasia Center, June 2019. https://www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation-2-0.

———. "Europe Is Starting to Tackle Disinformation. The U.S. Is Lagging." *Washington Post*, June 17, 2019. https://www.washingtonpost.com/opinions/2019/06/17/europe-is-starting-tackle-disinformation-us-is-lagging/.

Preskill, Hallie, Marcie Parkhurst, and Jennifer Splansky Juster. *Guide to Evaluating Collective Impact Supplement: Sample Questions, Outcomes, and Indicators*. Boston: FSG, 2014. https://www.collectiveimpactforum.org/sites/default/files/Guide%20to%20Evaluating%20CI%2003.pdf.

RAND. "Tools that Fight Disinformation Online." Accessed August 28, 2020. https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html.

Revishvili, Giorgi. "Two Sides of the Same Coin: Misinformation and Disinformation." Sunlight Foundation, May 23, 2019. https://sunlightfoundation.com/2019/05/23/two-sides-of-the-same-coin-misinformation-and-disinformation/.

Rosenberger, Laura, and J. M. Berger. "Hamilton 68: A New Tool to Track Russian Disinformation on Twitter." Alliance for Securing Democracy, August 2, 2017. https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/.

Sample, Char, Connie Justice, and Emily Darraj. "A Model for Evaluating Fake News." Paper presented at the CyCon U.S. 2018, Washington, DC, November 14–15, 2018. https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session4-Paper1.pdf?ver=2018-11-13-160900-603.

Schoen, Fletcher, and Christopher J. Lamb. *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*. Strategic Perspectives no. 11. Washington, DC: Institute for National Strategic Studies, 2012. https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

Singer, P. W., and Emerson Brooking. *LikeWar: The Weaponization of Social Media*. New York: Houghton Mifflin Harcourt, 2018. Kindle.

Spaulding, Suzanne, and Eric Goldstein. *Countering Adversary Threats to Democratic Institutions*. Washington, DC: Center for Strategic and International Studies, 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180214_Spaulding_CounteringAdversaryThreats_Web2.pdf?EzqGtMwOAjQIIH8eRNNoZ10T49OV63lh.

Spaulding, Suzanne, Devi Nair, and Arthur Nelson. *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System*. Washington, DC: Center for Strategic International Studies, 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf.

Stachowiak, Sarah, and Lauren Gase. "Does Collective Impact Really Make an Impact?" *Stanford Social Innovation Review*, August 2018. https://ssir.org/articles/entry/does_collective_impact_really_make_an_impact.

Sunstein, Cass R. *#Republic: Divided Democracy in the Age of Social Media*. Princeton, NJ: Princeton University Press, 2017.

Tamarack Institute. "Collective Impact." Accessed September 12, 2020. https://www.tamarackcommunity.ca/collectiveimpact.

———. *Collective Impact Self-Assessment and Planning Tool*. Waterloo, ON: Tamarack Institute, 2017. https://www.tamarackcommunity.ca/hubfs/Collective%20Impact/Tools/CI%20Self%20Assessment%20Tool.pdf?hsCtaTracking=8df74891-21af-4a7c-88d7-bb024f0d7d62%7C90f5999e-f7d9-4112-890e-96ed8a56a460.

Taylor, Margaret L. "Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe." *Techtank* (blog), July 31, 2019. https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*. Menlo Park, CA: Hewlett Foundation, 2018. https://hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf.

Tzu, Sun. *The Art of War*. Greyhound Press, 2017.

U.S. Congress. House of Representatives. *Statement of John Lansing CEO and Director U.S. Agency for Global Media before the House Appropriations Subcommittee on State, Foreign Operations, and Related Programs "United States Efforts to Counter Russian Disinformation and Malign Influence."* 116th Cong., 1st sess., July 10, 2019. https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-LansingJ-20190710.pdf.

———. *Statement of Lea Gabrielle Special Envoy & Coordinator for the Global Engagement Center, U.S. Department of State before the House Appropriations Subcommittee on State, Foreign Operations, and Related Programs "United States Efforts to Counter Russian Disinformation and Malign Influence."* 116th Cong., 1st sess., July 10, 2019. https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-GabrielleL-20190710.pdf.

———. *Statement of Nina Jankowicz Woodrow Wilson International Center for Scholars, Kennan Institute before the United States House Committee on Appropriations Subcommittee on State, Foreign Operations, and Related Programs concerning "United States Efforts to Counter Russian Disinformation and Malign Influence."* 116th Cong., 1st sess., July 10, 2019. https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-JankowiczN-20190710.pdf.

———. *Testimony Matthew Masterson Senior Cybersecurity Advisor Cybersecurity and Infrastructure Security Agency U.S. Department of Homeland Security for a Hearing on Securing America's Elections Part II: Oversight of Government Agencies before the United States House of Representatives Committee on the Judiciary.* 116th Cong., 1st sess., October 22, 2019. https://www.congress.gov/116/meeting/house/110106/witnesses/HHRG-116-JU00-Wstate-MastersonM-20191022.pdf.

———. *United States House Committee on Appropriations—Subcommittee on State, Foreign Operations, and Related Programs United States Efforts to Counter Russian Disinformation and Malign Influence*. 116th Cong., 1st sess., July 10, 2019. https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-PolyakovaA-20190710.pdf.

U.S. Congress. Senate. *Foreign Influence Operations and their Use of Social Media Platforms: Hearing before the Select Committee on Intelligence*. 115th Cong., 2nd sess., August 1, 2018. https://www.intelligence.senate.gov/sites/default/files/documents/os-rdiresta-080118.pdf.

———. *Statement of Laura Rosenberger Alliance for Securing Democracy, the German Marshall Fund of the United States before the United States Senate Select Committee on Intelligence Concerning "Foreign Influence Operations and their Use of Social Media Platform."* 115th Cong., 2nd sess., August 1, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/07/ROSENBERGER_SSCI-statement_Foreign-Influence-Ops-on-Social-Media_08-01-1....pdf.

———. *United States Senate Foreign Relations Subcommittee on State Department and USAID Management, International Operations, and Bilateral International Development Hearing on "The Global Engagement Center: Leading the United States Government's Fight against Global Disinformation Threat."* 116th Cong., 2nd sess., March 5, 2020. https://www.foreign.senate.gov/imo/media/doc/030520_Polyakova_Testimony.

———. *Written Testimony of Derek Slater Director, Information Policy, Google LLC United States Senate Committee on Commerce, Science, and Transportation "Mass Violence, Extremism, and Digital Responsibility."* 116th Cong., 1st sess., September 18, 2019. https://www.commerce.senate.gov/services/files/B74BE056-4446-470B-8B3C-F2E4463AFB66.

U.S. Senate Committee on Homeland Security and Governmental Affairs. "Peters, Portman Bill Responding to Growing Threat of Deepfakes Advances in Senate." July 26, 2019. https://www.hsgac.senate.gov/media/minority-media/peters-portman-bill-responding-to-growing-threat-of-deepfakes-advances-in-senate.

United States Census Bureau. "Census Bureau Report at Least 350 Languages Spoken in U.S. Homes." November 3, 2015. https://www.census.gov/newsroom/press-releases/2015/cb15-185.html.

Veljovski, Gjorgji, Nenad Taneski, and Metodija Dojchinovski. "The Danger of 'Hybrid Warfare' from a Sophisticated Adversary: The Russian 'Hybridity' in the Ukrainian Conflict." *Defense & Security Analysis* 33, no. 4 (2017): 292–307. https://doi.org/10.1080/14751798.2017.1377883.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (March 9, 2018): 1146–1151. http://www.sciencemag.org/lookup/doi/10.1126/science.aap9559.

Waltzman, Rand. *The Weaponization of Information: The Need for Cognitive Security*. CT-473. Santa Monica, CA: RAND, 2017. http://www.rand.org/pubs/testimonies/CT473.html.

Wardle, Claire, and Hossein Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Report Number DGI(2017)09. Strasbourg, France: Council of Europe, 2017. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Warner, Mark. "A New Doctrine for Cyberwarfare & Information Operations." Speech, Center for a New American Security, December 7, 2019. https://www.warner.senate.gov/public/index.cfm/2018/12/warner-calls-for-society.

Watts, Clint. *Messing with the Enemy*. New York: Harper, 2018. Kindle.

Weaver, Liz. "Navigating Collective Impact." *FSG* (blog). May 7, 2013. https://www.fsg.org/blog/navigating-collective-impact.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California