NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FAKE NEWS, CONSPIRACY THEORIES, AND LIES: AN INFORMATION LAUNDERING MODEL FOR HOMELAND SECURITY

by

Samantha M. Korta

March 2018

Co-Advisors: Rodrigo Nieto-Gomez
Lauren Wollman

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 March 2018	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE FAKE NEWS, CONSPIRACY THEORIES, AND LIES: AN INFORMATION LAUNDERING MODEL FOR HOMELAND SECURITY	5. FUNDING NUMBERS
6. AUTHOR(S) Samantha M. Korta	
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. IRB number ____N/A____.

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

13. ABSTRACT (maximum 200 words)

The purpose of this research, broadly speaking, is to expose the threat that "fake news" poses to our national security. This thesis answers the question: Can the information laundering model, or a modified version of it, be used to explain how the internet is exploited to spread fake news, and the resulting threat to the United States? I assert that a well-crafted narrative, whether true or false, can be spread rapidly online due to the accessibility and interconnectedness of the internet ecosystem. I then articulate how these narratives can be further accelerated and disseminated when propagandists take advantage of existing processes that improve the customization, ease of access, and availability of information online. I do this by modifying the information laundering model, and then using the new model to examine the interconnectedness of search engines, blogs, social networking platforms, and media/academic outlets, and how these connections can be exploited to launder false or purposefully misleading information into public discourse. Finally, I demonstrate how this process allows adversarial nations, criminals, and malicious actors to increase public discord, undermine democracy, and threaten Americans' physical and cognitive security.

14. SUBJECT TERMS fake news, information laundering, hybrid warfare, propaganda	15. NUMBER OF PAGES 153
	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.

FAKE NEWS, CONSPIRACY THEORIES, AND LIES: AN INFORMATION LAUNDERING MODEL FOR HOMELAND SECURITY

Samantha M. Korta
Fusion Center Deputy Director/Intelligence Supervisor,
Wisconsin Department of Justice—Division of Criminal Investigation
B.S., University of Wisconsin–Madison, 2007

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
March 2018

Approved by: Rodrigo Nieto-Gomez, Ph.D.
Co-Advisor

Lauren Wollman, Ph.D.
Co-Advisor

Erik Dahl, Ph.D.
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this research, broadly speaking, is to expose the threat that "fake news" poses to our national security. This thesis answers the question: Can the information laundering model, or a modified version of it, be used to explain how the internet is exploited to spread fake news, and the resulting threat to the United States? I assert that a well-crafted narrative, whether true or false, can be spread rapidly online due to the accessibility and interconnectedness of the internet ecosystem. I then articulate how these narratives can be further accelerated and disseminated when propagandists take advantage of existing processes that improve the customization, ease of access, and availability of information online. I do this by modifying the information laundering model, and then using the new model to examine the interconnectedness of search engines, blogs, social networking platforms, and media/academic outlets, and how these connections can be exploited to launder false or purposefully misleading information into public discourse. Finally, I demonstrate how this process allows adversarial nations, criminals, and malicious actors to increase public discord, undermine democracy, and threaten Americans' physical and cognitive security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

PROLOGUE: A BATTLEGROUND OF FEAR AND CURIOSITY.....1

I. THE HITCHHIKER'S GUIDE TO ALTERNATIVE FACTS.....23
- **A. PROBLEM STATEMENT.....23**
- **B. RESEARCH DESIGN.....28**

II. THE WAR (OF WORDS) TO END ALL WARS.....31
- **A. CONSPIRACY THEORIES.....31**
- **B. FAKE NEWS.....34**
- **C. PROPAGANDA.....35**
- **D. WEAPONIZED NARRATIVES AND COUNTERFEIT NARRATIVES.....44**
- **E. ETHOS, PATHOS, LOGOS, AND THE EFFECTIVENESS OF COUNTERFEIT NARRATIVES.....46**

III. ECHO CHAMBERS AND ADVERTISING AND BOTS ... OH MY!.....55
- **A. ECHO CHAMBERS.....60**
- **B. ONLINE ADVERTISING.....62**
- **C. BOTS AND COMPUTATIONAL PROPAGANDA.....66**
- **D. ADDITIONAL EMERGING TECHNOLOGIES.....71**

IV. INFORMATION LAUNDERING: OR HOW TO CHEAT THE SYSTEMS.....75
- **A. INFORMATION LAUNDERING: AN INTRODUCTION.....75**
- **B. INFORMATION LAUNDERING 2.0 MODEL.....79**
  - **1. Placement.....81**
  - **2. Layering.....83**
  - **3. Integration.....97**

V. HOW WE SAVE THE WORLD (AND OTHER USEFUL TIPS).....99
- **A. PREVENT PLACEMENT OF THE COUNTERFEIT NARRATIVE INTO THE SYSTEM.....101**
- **B. RE-LEGITIMIZE AND REINFORCE ENABLERS.....105**
- **C. SLOW DOWN THE ACCELERATORS.....106**
- **D. ATTACK THE AMPLIFIERS.....109**
- **E. INOCULATE AGAINST INTEGRATION.....112**

F. MAKE INFORMATION LAUNDERING A CRIME AND FACTUAL INFORMATION A RIGHT 114
G. GET EDUCATED AND DEMAND MORE.....117

LIST OF REFERENCES 121

INITIAL DISTRIBUTION LIST 131

LIST OF FIGURES

Figure 1. The Jowett and O'Donnell Purpose Model of Propaganda 41

Figure 2. Information Laundering 1.0 Model.....78

Figure 3. Information Laundering 2.0 Model.....81

Figure 4. Preventing a Counterfeit Narrative from Entering the System.....102

Figure 5. Re-legitimizing and Reinforcing Enablers.....105

Figure 6. Slowing down the Accelerators 107

Figure 7. Attacking the Amplifiers.....110

Figure 8. Inoculating against Integration 112

Figure 9. Criminalizing Information Laundering.....115

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY OF TERMS

Accelerators: online mechanisms, including but not limited to echo chambers, online advertising, and computational propaganda, used during information laundering to make the process itself more effective, efficient, and in many cases profitable.

Amplifiers: secondary actors engaged in information laundering who do not necessarily create their own campaign, but instead seek to exploit existing unrest or confusion created by the primary actors, either for ideological or financial purposes.

Availability heuristic: the concept that individuals judge the likelihood, frequency, and extremity of incidents or events based on the ease with which those examples come to mind.[1]

Backfire effect: a tendency for an individual to fight back and reject, rather than consider, information being presented if it contradicts his or her belief.[2]

Belief perseverance: the tendency for individuals to defend the beliefs they currently hold and subconsciously weigh evidence that supports those beliefs more heavily.[3]

Bot: a piece of code that can run automated tasks.

Botnet: a group of bots that are created and centrally controlled by a master, called a botmaster.[4]

Computational propaganda: "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks."[5]

---

[1] Amos Tversky and Daniel Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology* 5 (1973): 207–232, https://msu.edu/~ema/803/Ch11-JDM/2/TverskyKahneman73.pdf.

[2] (Stephan Lewandowsky et. al, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (December 2012): 106–131, https://doi.org/10.1177/1529100612451018.

[3] Raymond S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology* 2, no. 2 (1998): 175–220, http://psy2.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf.

[4] Juan Echeverría and Shi Zhou, "The 'Star Wars' Botnet with >350k Twitter Bots," Cornell University Library, June 13, 2017, https://arxiv.org/abs/1701.02405.

[5] Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary" (working paper, University of Oxford, 2017), 3, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Confirmation bias: a phenomenon by which an individual, usually without being aware of it, weighs information or evidence that supports his or her prior-held beliefs and discounts information or evidence that is inconsistent with his or her prior beliefs.[6]

Conspiracy theory: "the belief that an organization made up of individuals or groups was or is acting covertly to achieve some malevolent end."[7]

Counterfeit narrative: online content, or a series of content, created for the purposes of information laundering. The content benefits the propagandist and has a negative or destructive effect on the recipient of that narrative.

Deepfake: a fake pornography video that swaps the faces of pornography stars with those of celebrities.[8]

Disinformation: "false, incomplete, or misleading information that is passed, fed, or confirmed to a targeted individual, group, or country."[9]

Echo chamber: the metaphorical term describing when a user enters into a situation online in which he or she consumes only content that agrees with his or her existing viewpoint, thus reinforcing that viewpoint.[10]

Enablers: theoretical domains that allow the interconnectedness of the internet to be depicted and the virality and spread of information to be visualized during information laundering.

Fake news: "hoax-based stories that perpetuate hearsay, rumors, and misinformation."[11]

---

[6] Nickerson, "Confirmation Bias."

[7] Michael Barkun, *A Culture of Conspiracy: Apocalyptic Visions in Contemporary America (Comparative Studies in Religion and Society)*, 2nd edition (Berkeley: University of California Press, 2013), https://www.amazon.com/dp/B00DNJD46C/ref=docs-os-doi_0.

[8] Samantha Cole, "Fake Porn Makers Are Worried about Accidentally Making Child Porn," *Motherboard*, February 27, 2018, https://motherboard.vice.com/en_us/article/evmkxa/ai-fake-porn-deepfakes-child-pornography-emma-watson-elle-fanning.

[9] H.R. Shultz and R. Godson, *Dezinformatsia: Active Measures in Soviet strategy* (Washington, DC: Pergamon Brassey's, 1984)

[10] Seth Flaxman, Sharad Goel, and Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly* 80, Special Issue (2016).

[11] 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, http://journals.sagepub.com/doi/abs/10.1177/0002764217701217.

False consensus effect: a cognitive bias in which people attribute others' views to their own, overestimating the extent to which their views are held in the larger population.[12]

Hybrid warfare: "a form of warfare in which one of the combatants bases its optimized force structure on the combination of all available resources—both conventional and unconventional—in a unique culture context to produce specific, synergistic effects against a conventionally-based opponent."[13]

Implicit egotism: the tendency for recipients to more likely believe messages when they are being delivered by someone they perceive as being similar to themselves.[14]

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."[15]

Integration: the phase during information laundering when a counterfeit narrative becomes part of public discourse and knowledge.

Layering: the phase of information laundering when the counterfeit narrative is laundered through a series of domains and connections until it has reached a virality and veracity that opens it up for public discourse without the original source or motive being understood.

MADCOMs: "the integration of [artificial intelligence] systems into machine-driven communications tools for use in computational propaganda."[16]

Placement: the phase during information laundering when the messaging is crafted into a counterfeit narrative and placed into the internet ecosystem.

---

[12] Magdalena Wojcieszak and Vincent Price, "What Underlies the False Consensus Effect? How Personal Opinion and Disagreement Affect Perception of Public Opinion," *International Journal of Public Opinion Research* 21, no. 1 (March 2009): 25–46, https://doi.org/10.1093/ijpor/edp001.

[13] Timothy B. McCulloh and Richard B. Johnson, *Hybrid Warfare*, JSOU Report 13-4 (MacDill AFB, FL: JSOU, 2013), 17

[14] Matt Chessen, "Understanding the Psychology behind Computational Propaganda," in *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, ed. Shaun Powers and Markos Kounalakis (Washington, DC: United States Advisory Commission on Public Diplomacy, 2017).

[15] Adam Klein, "Slipping Racism into the Mainstream: A Theory of Information Laundering," *Communication Theory* 22, no. 4 (November 2012): 427–448.

[16] Matt Chessen, *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, And Threaten Democracy ... And What Can Be Done about it* (Washington, DC: Atlantic Council, 2017), 6, http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.

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."[17]

Technical ethos: the credibility that comes from being proficient in developing professional-looking webpages.[18]

Weaponized narrative: content made to "deploy in a rapid-fire series of mutually-reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal cost."[19]

---

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

[18] Shane Borrowman, "Critical Surfing: Holocaust Denial and Credibility on the Web," *College Teaching* 47, no. 2 (Spring 1999): 44–47.

[19] Jon Herrmann, "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War," *The Strategy Bridge*, July 27, 2017, https://thestrategybridge.org/the-bridge/2017/7/27/nine-links-in-the-chain-the-weaponized-narrative-sun-tzu-and-the-essence-of-war.

EXECUTIVE SUMMARY

Today, citizens must navigate an online ecosystem wherein the pathways used to find true information are the same as those used to find false information. These pathways have also been usurped by both "non-state and state actors who aim not only to disseminate misinformation but, most damaging, to erode trust in traditional sources of information."[1] This has created a political, national, and homeland security environment that often calls into question the very nature of truth and reality. What's more, outrageous conspiracy theories, once ascribed to the fringes of society, are now being normalized and incorporated into mainstream dialogues. When people talk about this problem, however, they typically point to social media, or even specifically to a social media platform like Facebook or Twitter, as if social media are solely responsible for the degradation of truth. While these platforms do seem to play a role, the internet itself has become a social platform and, through the dynamism and instructiveness of almost all websites, apps, and internet platforms, a new global infrastructure for communication, sharing, and outrage has formed. This has created an online space that, for its complex, interconnected ecosystem, requires a new paradigm for human understanding of truth and cognitive security.

In 2012, one researcher—Adam Klein—recognized the potential role the totality of the internet plays in normalizing racist rhetoric; through his foundational work, we can begin to see a framework for understanding the phenomenon we are facing. In Klein's original model, information laundering is described as the process by 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."[2] Taking into account the amalgamation of conspiracy theories, "fake news," propaganda, and weaponized narratives spouted by extremist groups, combined with technological

[1] Bruce Wharton, "Remarks on 'Public Diplomacy in a Post-truth Society,'" in *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, ed. Shaun Powers and Markos Kounalakis (Washington, DC: United States Advisory Commission on Public Diplomacy, 2017), 7–8.

[2] Adam Klein, "Slipping Racism into the Mainstream: A Theory of Information Laundering," *Communication Theory* 22, no. 4 (November 2012): 429.

advancements and a growing awareness of propaganda's effectiveness, it is perhaps time to modify this model. This thesis therefore proposes the Information Laundering 2.0 model.

This research demonstrates how the interconnectedness of various internet platforms, coupled with existing and emerging online technologies, can be exploited to launder false or purposefully misleading information into public discourse at a volume and velocity previously unimaginable. It is important to study this phenomenon because this ongoing threat continues to raise difficult discussions among homeland security professionals, policymakers, and the general public, often creating an uncomfortable dialogue in which partisanship, freedom of speech, and privacy laws come into play. Nonetheless, establishing a practical framework, the Information Laundering 2.0 model, to help explain this phenomenon is a crucial step toward effective and sustainable actions to combat it.

Beginning with a foundation of propaganda research, this thesis builds a new concept, dubbed counterfeit narrative, to define the content of the propaganda being spread online. The counterfeit narrative concept helps explain the flawed nature of this information and accounts for the potential actors who could leverage its use, including nation-states, terrorist organizations, domestic extremists, and even corporations engaging in disingenuous advertising campaigns. 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.

Additionally, the current internet ecosystem, including the ease with which a consumer can both find and contribute to information, creates a very influential environment. It allows truthful, important information to spread at previously impossible rates, but at the same time opens up the floodgates for the rapid spread of counterfeit narratives. Propagandists can use online technologies such as computational propaganda, echo chambers, and advertising to further cheat the internet ecosystem and create and spread content that is more influential and believable. Committed actors can leverage these techniques to intentionally undermine the credibility of legitimate sources by leveling the playing field for subversive, often extremist, content that masquerades as credible content in the public debate.

Information Laundering 2.0 considers the concepts of counterfeit narrative and accelerators (technologies used to spread counterfeit narratives faster), as well as the internet ecosystem itself and the actors who take advantage of existing propaganda campaigns. The model is broken into three phases: placement, layering, and integration. The placement phase prepares the information, in the form of a counterfeit narrative, for maximum impact before it is placed into the internet ecosystem. Next, in the layering phase, the counterfeit narrative is laundered through a series of domains and connections until it has reached a virality and veracity that opens it up for public discourse, without the original source or motive being understood. During the layering phase, the propagandist may take advantage of accelerators—in the form of online advertising, computational propaganda, and echo chambers—in an effort to speed up the impact of the process. Additionally, amplifiers, or actors who enhance the campaigns of other information launderers for either ideological or financial purposes, may also come into play during the layering phase. Upon successful laundering, the narrative enters the integration phase and becomes part of public discourse and knowledge.

While the Information Laundering 2.0 model does not offer a simple, step-by-step solution for combating this complex problem, it helps frame the issue in a way that homeland security professionals, law enforcement, policymakers, and the general public can understand. It leverages real-world solutions at multiple levels while protecting free speech, and without sacrificing our nation's cognitive security. The Information Laundering 2.0 model should be the framework used and understood when addressing global, governmental, societal, and individual responses to this continuous threat. We must identify solutions that address the problem at every phase (placement, layering, and integration) and through every piece (enablers, accelerators, and amplifiers).

Any proposed solutions for combatting information laundering should be considered with a multi-level, multi-disciplinary, and multi-sector approach. This research should therefore not be seen as the definitive guide to ending information laundering, but only as a place to start the conversation, start the research, and start the response. Solutions to be considered include identifying strategies to prevent counterfeit narratives from entering the online ecosystem altogether, rebuilding trust and legitimacy of online

institutions, slowing down the technology that speeds up counterfeit narratives, limiting malicious actors' ability to amplify existing campaigns for either ideological or financial purposes, and inoculating the public against information laundering before it happens. Further, from a holistic perspective, considering access to truthful information as a right and information laundering itself as a crime may help combat the issue. Finally, restructuring our education system and the public's awareness, especially as it relates to consumption of sources online, is also important.

The United States must immediately recognize and seek to understand the concepts of counterfeit narratives and information laundering, as well as the threats they pose to democracy, freedom, and homeland security. Policymakers should tackle these issues with laws that are not too broad to limit free speech or freedom of the press, but effective enough to provide citizens with their right to be "secure in their persons" by establishing and defending cognitive security. Meanwhile, law enforcement and homeland security officials should make efforts to prepare for, and help mitigate, the confusion and tension that ultimately arise from these narratives and prepare to protect themselves and the general public from incidents that, without intervention, could escalate to violence.

ACKNOWLEDGMENTS

This thesis has been an incredibly difficult, rewarding, and wonderful journey. First and foremost, I have to thank my wonderful and patient fiancé for supporting me throughout this program. I could not have completed it without his support, as well as the support of my family and friends. Thank you to my amazing parents, who love and support me and who taught me how to be dedicated and determined.

Thank you to all the wonderful staff at the Center for Homeland Defense and Security who helped my fellow classmates and me through this journey. To Lauren Fernandez, who taught me about "type two fun" and steered me in the right direction from the very start. To Chris Bellavita, who encouraged me to explore where there be dragons. To Erinn, who kept my fellow classmates and me sane throughout this entire process. To Aileen Houston, who may in fact be a super hero and the most amazing editor in existence. And most importantly, to Lauren Wollman and Rodrigo Nieto-Gomez, for being inspirational, dedicated, and supportive advisors who were there with me every step of the way.

Thank you to the amazing and hard-working staff at the Wisconsin Statewide Intelligence Center who supported me through this program and allowed me to have this once-in-a-lifetime opportunity. To my friend and mentor, Bob K, who helps me become a better leader, a better citizen, and a better person each and every day.

And finally, thank you to my fellow classmates. The most eclectic, impressive, and amazing group of individuals, who I have had the pleasure of getting to know over the past 18 months. 1611 for life!

THIS PAGE INTENTIONALLY LEFT BLANK

PROLOGUE: A BATTLEGROUND OF FEAR AND CURIOSITY

SCENE 1

February 1998: Andrew Wakefield, a former gastroenterologist who later became "one of the most reviled doctors of his generation," publishes a falsified report in *The Lancet* on the potential link between the measles, mumps, and rubella (MMR) vaccine and autism.[1] This research is quickly refuted and ultimately debunked by the rest of the medical community.[2] The journal eventually retracts the article, but lingering doubts and conspiracy theories about vaccinations persist. These conspiracy theories are widely spread online, most frequently on Facebook by females from both sides of the political aisle. In 2017, Smith and Graham conduct a study of this movement on Facebook and conclude that although the number of women sharing this information is small, social media may have "a role in spreading anti-vaccination ideas and making the movement durable on a global scale."[3] Millions of people have stopped vaccinating, leading to a 2008 measles endemic in the United Kingdom, a mumps outbreak in 2011 at Berkeley, and a measles crisis in Minnesota in 2017, just to name a few.[4] In fact, Gavi, the Vaccine Alliance, maintains a database and map of all outbreaks in the world and reports that since 2008, over 1.5 million measles cases that could have been prevented through vaccination have occurred.[5]

---

[1] Daniel Jolley and Karen M. Douglas, "The Effects of Anti-vaccine Conspiracy Theories on Vaccination Intentions," *PloS One* 9, no. 2 (February 2014): 1, https://doi.org/10.1371/journal.pone.0089177; Susan Dominus, "The Crash and Burn of an Autism Guru," *New York Times*, April 20, 2011, https://www.nytimes.com/2011/04/24/magazine/mag-24Autism-t.html.

[2] T. S. Sathyanarayana Rao and Chittaranjan Andrade, "The MMR Vaccine and Autism: Sensation, Refutation, Retraction, and Fraud," *Indian Journal of Psychiatry* 53, no. 2 (April 2011): 95–96, https://doi.org/10.4103/0019-5545.82529.

[3] Naomi Smith and Tim Graham, "Mapping the Anti-vaccination Movement on Facebook," *Information, Communication and Society* (December 2017): 1–18, https://doi.org/10.1080/1369118X.2017.1418406.

[4] "Anti-Vaxxers Brought Their War to Minnesota—Then Came Measles," *Wired*, May 7, 2017, https://www.wired.com/2017/05/anti-vaxxers-brought-war-minnesota-came-measles/; Jolley and Douglas, "Anti-vaccine Conspiracy Theories," 1; Alexandra Sifferlin, "Here Are Some Diseases We're Seeing Thanks to Anti-Vaxxers," *Time*, March 17, 2014, http://time.com/27308/4-diseases-making-a-comeback-thanks-to-anti-vaxxers/.

[5] "Vaccine-Preventable Disease Outbreaks," Vaccines Work, accessed March 3, 2018, http://www.vaccineswork.org/vaccine-preventable-disease-outbreaks/.

SCENE 2

February 2007: Illinois Senator Barack Obama announces his candidacy for the presidency of the United States.[6] Not long after, a movement attempting to undermine the legitimacy of his presidential campaign alleges that the candidate is not a U.S. citizen. Even though these claims originated on a white supremacist website, they become an active topic in mainstream discourse for years to follow.[7] Despite eventual evidence of Obama's citizenship (both his long- and short-form birth certificates from the state of Hawaii), the movement, dubbed the "birther movement," continues well into his presidency, and remains a contentious issue for many today.[8]

---

[6] "Illinois Sen. Barack Obama's Announcement Speech," *Washington Post*, February 10, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/02/10/AR2007021000879.html.

[7] Adam Klein, "Slipping Racism into the Mainstream: A Theory of Information Laundering," *Communication Theory* 22, no. 4 (November 2012): 427–48.

[8] Forty-Fourth U.S. President Barack Obama was born in Honolulu, Hawaii. "President Obama's Long Form Birth Certificate," whitehouse.gov, April 27, 2011, https://obamawhitehouse.archives.gov/blog/2011/04/27/president-obamas-long-form-birth-certificate; Kyle Dropp and Brendan Nyhan, "It Lives. Birtherism Is Diminished but Far from Dead," *New York Times*, September 23, 2016, www.nytimes.com/2016/09/24/upshot/it-lives-birtherism-is-diminished-but-far-from-dead.html.

SCENE 3

December 2012: Adam Lanza, a 20-year-old male, enters Sandy Hook Elementary School in Newtown, Connecticut, and opens fire, killing six adults and twenty children before ultimately taking his own life.[9] After the shooting, the parents of the deceased victims receive countless harassing messages and death threats from several individuals who believe the whole incident to be a "false flag" or even a hoax promulgated by "crisis actors" hired by the United States government.[10] Online conspiracy theorists perpetuate this false narrative after almost every mass casualty event, often claiming crisis actors have been hired to take part in a widespread government conspiracy across jurisdictions and national governments.

---

[9] "Connecticut State Police Sandy Hook Elementary School Shooting Reports," State of Connecticut, accessed January 15, 2018, http://cspsandyhookreport.ct.gov/; Stephen J. Sedensky III, "Report of the State's Attorney for the Judicial District of Danbury on the Shootings at Sandy Hook Elementary School" (report, State of Connecticut Division of Criminal Justice, 2013), http://www.ct.gov/csao/lib/csao/Sandy_Hook_Final_Report.pdf; State of Connecticut Office of the Child Advocate, "Shooting at Sandy Hook Elementary School" (report, State of Connecticut, 2014), http://www.ct.gov/oca/lib/oca/sandyhook11212014.pdf; "Sandy Hook Elementary Shooting: What Happened?," CNN, accessed January 17, 2018, http://www.cnn.com/interactive/2012/12/us/sandy-hook-timeline/index.html.

[10] Mike Wendling, "Sandy Hook to Trump: 'Help Us Stop Conspiracy Theorists,'" BBC News, April 2, 2017, http://www.bbc.com/news/blogs-trending-39194035; Barbara Demick, "In an Age of 'Alternative Facts,' a Massacre of Schoolchildren Is Called a Hoax," *Los Angeles Times*, February 3, 2017, www.latimes.com/nation/la-na-sandy-hook-conspiracy-20170203-story.html.

SCENE 4

August 2014: An internet culture war dubbed Gamergate erupts over the inclusion of women in the gaming industry.[11] Women in this industry are targeted by internet trolls, often receiving rape threats, death threats, and other harassing comments.[12] These threats are often so specific and graphic that victims are forced to flee their homes; law enforcement, including the FBI, investigates several of the claims as "criminally punishable" threats.[13]

---

[11] Caitlin Dewey, "The Only Guide to Gamergate You Will Ever Need to Read," *Washington Post*, October 14, 2014, https://www.washingtonpost.com/news/the-intersect/wp/2014/10/14/the-only-guide-to-gamergate-you-will-ever-need-to-read/.

[12] Dewey.

[13] Dewey.

SCENE 5

June 2014: Jerad and Amanda Miller open fire upon and kill two law enforcement officers who are having lunch at a CiCi's pizza in Las Vegas.[14] The couple then proceeds across the street to Walmart, where they kill a patron who attempts to intervene.[15] Jerad and Amanda are later described as having harbored "anti-government ideology" and holding strong conspiracy theory views, such as the U.S. government's use of "chemtrails"; it is believed that this sentiment played a role in their escalation to violence.[16]

---

[14] Matthew Walberg and Michael Muskal, "Dad of Female Las Vegas Shooter Begged Her Not to Marry Jerad Miller," *Los Angeles Times*, June 9, 2014, http://www.latimes.com/nation/nationnow/la-na-amanda-jared-miller-father-las-vegas-shooting-20140609-story.html.

[15] Walberg and Muskal.

[16] Walberg and Muskal; "Rejected by the Revolution, Jerad and Amanda Miller Decided to Start Their Own," *Las Vegas Review-Journal*, June 15, 2014, https://www.reviewjournal.com/news/bundy-blm/rejected-by-the-revolution-jerad-and-amanda-miller-decided-to-start-their-own/; Cynthia Johnston, "Killers of Las Vegas Cops Harbored Anti-government Ideology," Reuters, June 9, 2014, www.reuters.com/article/us-usa-nevada-shooting/killers-of-las-vegas-cops-harbored-anti-government-ideology-police-idUSKBN0EK1U320140609.

SCENE 6

August 2014: In the early hours of the morning, a 6.0 magnitude earthquake strikes Napa, California.[17] The earthquake awakens many in the Bay Area, who immediately take to social media, especially Twitter, to circulate information using the #NapaQuake and #NapaEQ hashtags.[18] These globally trending hashtags are soon hijacked by Twitter trolls, who inject their own messages.[19] The main injected content is related to accusations of military misconduct, including graphic images of torture and mangled bodies.[20] Most of the hijacked content seems to have originated from outside the United States.[21] These malicious activities make it difficult for residents or their loved ones to track the facts and identify crucial information in this time of crisis.

---

[17] Social Media Working Group for Emergency Services and Disaster Management (SMWGESDM), "Countering Misinformation, Rumors, and False Information on Social Media before, during, and after Disasters and Emergencies." Department of Homeland Security, March 2018, https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf.

[18] SMWGESDM.

[19] SMWGESDM.

[20] SMWGESDM.

[21] SMWGESDM.

SCENE 7

March 2015: The Brookings Institute, a non-partisan think tank headquartered in Washington, DC, releases an analysis of the individuals who support the Islamic State, known as ISIL or ISIS, on Twitter.[22] During the course of its research, Brookings found that ISIS may have used as many as 70,000 accounts to spread propaganda and messaging.[23] Accounts supporting ISIS had, on average, approximately 1,000 followers each, which is above average for a Twitter account, and were more active than the average Twitter account.[24] ISIS is also known to co-opt trending hashtags on social media and insert its own propaganda and violent imagery. This means that a child logged onto Twitter who clicks on the hashtag #AskRicky, in an effort to send a question to YouTube star Ricky Dillon, may instead be confronted with messages such as, "As you kill us, we are killing you."[25] Despite overwhelming evidence that extremist material continues to grow online, there is a lack of consensus on the role (if any) the internet plays on individual radicalization to violent extremism and terrorism.[26] However, while experts do not yet agree on the degree to which these campaigns can radicalize individuals, many argue that, at the very least, these social media campaigns do generate support for the terrorist group, inspire homegrown violent extremists, and mobilize foreign fighters to travel abroad.[27]

---

[22] J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter" (analysis paper no. 20, Brookings, 2015), www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

[23] Berger and Morgan, 7:1.

[24] Berger and Morgan, 7:3.

[25] Casey Johnston, "ISIS Co-opts Twitter Hashtags to Spread Threats, Propaganda," Ars Technica, August 26, 2014, https://arstechnica.com/information-technology/2014/08/isis-co-opts-twitter-hashtags-to-spread-threats-propaganda/.

[26] Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research," *Studies in Conflict and Terrorism* 40, no. 1 (January 2, 2017): Foreword.

[27] "[Homegrown violent extremists (HVEs)] who mobilize to engage in violence are often inspired to act without receiving direct operational support from a [foreign terrorist organization]. Alternatively, their mobilization to violence can be enabled and often sped up by contact, typically via the internet or social media, with terrorist groups who provide operational guidance but leave overall control of the operation to the HVE." Countering Violent Extremism Task Force, "Reference Aid: ISIS and Al-Qa'ida-Inspired Homegrown Violent Extremists," Department of Homeland Security, September 2017, www.dhs.gov/sites/default/files/publications/ISIS%20and%20AQ-Inspired%20Violent%20Extremists_CVE%20Task%20Force_Final.pdf.

SCENE 8

March 2016: The Microsoft Corporation launches "Tay," an experimental Twitter bot that uses artificial intelligence to learn from interactions with other Twitter users. Tay is given the personality profile of an American female, aged 18–24, with interests in pop culture and other topics relevant to the millennial demographic.[28] Within sixteen hours, Tay begins to spout conspiracy theories about 9/11, using explicit profanity, and promoting Nazism.[29] Tay also tweets expletives at Zoe Quinn, a videogame designer and activist who was one of the primary targets in the controversial Gamergate incidents.[30] Tay is pulled offline. When Tay is later reinstated, she is quickly removed again due to similar abuses. Nonetheless, from March 23 through April 6, 2016, Tay generates "approximately 93,000 tweets and 189,000 followers."[31]

---

[28] Gina Neff and Peter Nagy, "Automation, Algorithms, and Politics | Talking to Bots: Symbiotic Agency and the Case of Tay," *International Journal of Communication Systems* 10 (October 2016): 4921, http://ijoc.org/index.php/ijoc/article/view/6277/1804.

[29] Neff and Nagy; Davey Alba et al., "It's Your Fault Microsoft's Teen AI Turned into Such a Jerk," *Wired*, March 25, 2016), https://www.wired.com/2016/03/fault-microsofts-teen-ai-turned-jerk/.

[30] Neff and Nagy, "Talking to Bots."

[31] Neff and Nagy, 4923.

SCENE 9

December 2016: In response to a conspiracy theory originating from Reddit and 4Chan, and promulgated by InfoWars, an armed gunman enters a local pizza joint in Washington, DC, to "self-investigate" a "secret pedophilia dungeon" reportedly run by Bill and Hillary Clinton in the establishment's basement.[32] The gunman fires three shots into the restaurant, but luckily no one is injured or killed, and the suspect is arrested without incident. This conspiracy theory, dubbed Pizzagate, continues to promulgate across the internet despite the fact that the armed gunman did not locate a sex trafficking ring, and despite the absence of any evidence that he actually would have. In fact, the restaurant associated with the alleged activity does not even have a basement.[33] Nonetheless, this online conspiracy theory continues to spread and results in a real-life public safety concern, one that could have ended very differently.

---

[32] Reddit and 4Chan are online discussion platforms where users discuss news, interests, and other topics. InfoWars is an online entertainment channel hosted by Alex Jones, a boisterous personality known for perpetuating conspiracy theories. German Lopez, "Pizzagate, the Fake News Conspiracy Theory That Led a Gunman to DC's Comet Ping Pong, Explained," Vox, December 5, 2016, https://www.vox.com/policy-and-politics/2016/12/5/13842258/pizzagate-comet-ping-pong-fake-news; Christina Cauterucci, Jonathan L. Fischer and Will Oremus, "Comet Is D.C.'s Weirdo Pizza Place. Maybe That's Why It's a Target," *Slate*, December 6, 2016, http://www.slate.com/blogs/outward/2016/12/06/comet_ping_pong_is_a_haven_for_weirdos_and_now_a_target.html; Andrew Breiner, "Pizzagate, Explained: Everything You Want to Know about the Comet Ping Pong Pizzeria Conspiracy Theory but Are Too Afraid to Search for on Reddit," *Salon*, accessed May 14, 2017, http://www.salon.com/2016/12/10/pizzagate-explained-everything-you-want-to-know-about-the-comet-ping-pong-pizzeria-conspiracy-theory-but-are-too-afraid-to-search-for-on-reddit/; Reddit, accessed February 4, 2018, https://www.reddit.com/; 4chan, accessed February 4, 2018, https://www.4chan.org/; Infowars, accessed September 11, 2017, https://www.infowars.com/.

[33] Gregor Aisch, Jon Huang, and Cecilia Kang, "Dissecting the #PizzaGate Conspiracy Theories," *New York Times*, December 10, 2016, www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html.

SCENE 10

January 6, 2017: The Office of the Director of National Intelligence releases a declassified intelligence report, which finds that an influence campaign had been ordered by Russian President Vladimir Putin before the 2016 presidential election in an attempt to undermine faith in the American democratic process.[34] The report states:

> Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."[35]

During the election cycle, Russia-based media outlets openly supported candidate Donald Trump and consistently argued that he was the target of an unfair and biased mainstream media that was catering to corrupt political officials.[36] Those same Russian outlets cast candidate Hillary Clinton in a consistently negative light, denigrating her physical and mental health and accusing her of corruption. Additionally, paid internet trolls out of the Saint Petersburg–based Internet Research Agency further amplified the narratives. The United States Intelligence Community considers this the boldest influence effort ever conducted by the Russian government, at least in the United States, and believes this behavior will continue into the foreseeable future.[37]

Also during the election cycle, Veles, Macedonia, a small town of roughly 44,000 to 55,000 citizens, became a hotbed for the manufacture and dissemination of "fake news."[38] Veles churned out thousands of fake articles; the young Macedonians who

---

[34] Office of the Director of National Intelligence (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections* (Washington, DC: ODNI, 2017), ii.

[35] ODNI.

[36] ODNI, 4.

[37] ODNI, 5.

[38] Samanth Subramanian, "Inside the Macedonia Fake-News Complex," *Wired*, February 15, 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news/; "The Fake News Machine: Inside a Town Gearing up for 2020," CNN, accessed September 14, 2017, http://money.cnn.com/interactive/media/the-macedonia-story/; Dan Tynan, "How Facebook Powers Money Machines for Obscure Political 'News' Sites," *Guardian*, August 24, 2016, http://www.theguardian.com/technology/2016/aug/24/facebook-clickbait-political-news-sites-us-election-trump; Craig Silverman and Lawrence Alexander, "How Teens in the Balkans Are Duping Trump Supporters with Fake News," BuzzFeed, accessed October 12, 2017, https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

propagated the lies earned thousands of dollars a week (the average salary for a Macedonian citizen is under $500 per month).[39] These websites featured headlines like "Hillary's Illegal Email Just Killed its First American Spy" and "This Is How Liberals Destroyed America."[40] The websites were registered with American-sounding domain names—such as WorldPoliticus.com, TrumpVision365.com, USConservativeToday.com, DonaldTrumpNews.co, and USADailyPolitics.com—to further sow confusion about the sites' origins.[41] One young Macedonian entrepreneur reported to *Wired* magazine that the majority of the time, due to his fractured English, he did not even create the articles he disseminated; he simply re-disseminated stories from websites in America "which manufactured white-label falsehoods disguised as news on an industrial scale."[42] This new information enterprise became a primary, and very lucrative, source of income for many Veles youth, who often posted under bogus Facebook profiles disguised to look like American accounts.[43] Domestically, a much smaller but still lucrative two-person site operating out of a home in the San Francisco Bay Area generated anywhere from $10,000 to $40,000 per month through ads running along their hyperpartisan website.[44]

Since the election, Facebook and Google have begun blocking these kinds of websites. But their efforts will likely not stop this kind of activity, especially with individuals like Mirko Ceselkoski, who now trains Macedonians to conduct their own fake news operations.[45]

---

[39] Subramanian, "Inside the Macedonia Fake-News Complex"; CNN, "The Fake News Machine"; Tynan, "Facebook Money Machines"; Silverman and Alexander, "Teens in the Balkans."

[40] Tynan, "Facebook Money Machines."

[41] Silverman and Alexander, "Teens in the Balkans."

[42] Subramanian, "Inside the Macedonia Fake-News Complex."

[43] Subramanian.

[44] Tynan, "Facebook Money Machines."

[45] CNN, "The Fake News Machine."

SCENE 11

May 2017: A meme featuring photographs of young women crying at the Aurora, Colorado, movie theater shooting (July 20, 2012); Sandy Hook Elementary School shooting (December 14, 2012); Roseburg, Oregon, Community College shooting (October 1, 2015); Boston Marathon bombing (April 15, 2013); and later the Manchester bombing (May 22, 2017) is reported to depict the same female, a "crisis actor" hired to help the conspiring parties (the U.S. and British governments) perpetuate these "false flags" as actual attacks.[46] The claim is investigated and proven false; nonetheless, the disinformation continues to spread.[47] Proponents of this conspiracy theory proclaim:

> Powerful forces in your own government have set up operations to terrorize and kill you and to blame it on a foe of their convenience, in order to further a political agenda that will destroy what's left of your Constitutional freedoms and enslave you.[48]

---

[46] "FACT CHECK: Crisis Actors Uncovered?," Snopes, May 28, 2017, http://www.snopes.com/same-girl-crying-now-oregon/.https://www.truthorfiction.com/sandy-hook-shooting-conspiracy-theory/.

[47] Snopes, "Crisis Actors Uncovered"; Wendling, "Sandy Hook to Trump."

Author's note: Snopes said the claim was false, but truthorfiction.com claims it is "unproven" rather than "false" because most of the claims were based only on "personal opinions that cannot be definitely proven true or false."

[48] Johnny Cirucci, "What REALLY Happened at Sandy Hook?," J*ohnny Cirucci* (blog), December 21, 2013, http://johnnycirucci.com/what-really-happened-at-sandy-hook/.

SCENE 12

August 2017: From April 27 to August 30, 2017, the Federal Communications Commission (FCC) opens up its online forums for public comments related to the new net neutrality regulation proposals.[49] Over 21 million comments are submitted, a staggering increase from the 450,000 that were submitted during a similar comment window in 2014.[50] At first glance, most comments appear to be against net neutrality regulation. However, an analysis by the Pew Research Center, a nonpartisan American think tank, reveals important use of false, misleading, and/or recycled personal information in 57 percent of the posts, evidence of organized information campaigns attempting to flood the forum with duplicate messages, and thousands of comments submitted at the same time.[51] Further, trolls used the identities of real individuals, posting under their names without their knowledge.[52]

---

[49] Paul Hitlin, Kenneth Olmstead, and Skye Toor, *Public Comments to the Federal Communications Commission about Net Neutrality Contain Many Inaccuracies and Duplicates* (Washington, DC: Pew Research Center, 2017), 2, http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/11/30155447/PI_2017.11.29_Net-Neutrality-Comments_FINAL.pdf.

[50] Hitlin, Olmstead, and Toor, 2.

[51] Hitlin, Olmstead, and Toor, 3.

[52] "IRL: Online Life Is Real Life – Bot or Not," RadioPublic video, accessed January 17, 2018, 28:10, https://play.radiopublic.com/irl-online-life-is-real-life-6Bv5Op/ep/s1!92721f1be13eba2236 55f6ada2b978c38692216b.

SCENE 13

August 2017: Former pharmaceutical executive and hedge fund manager Martin Shkreli is accused of using social media and blogs to attack biotech companies in an effort to manipulate share prices.[53] Around 2011, Shkreli reportedly used stock blogging websites, social media, and misstated material facts to cast doubt on small publicly traded companies in an effort to create panic and induce stockholders to sell, thus decreasing the value of the company.[54] So, instead of using social media to report on a company that legitimately should be short-saled, Shkreli created negative attention on that company through his reports, which "lacked rigor and accountability."[55]

---

[53] "The Business of Disinformation: A Taxonomy Fake News Is More than a Political Battlecry," Digital Shadows, accessed March 26, 2018, 7, http://info.digitalshadows.com/rs/457-XEY-671/images/DigitalShadows-TheBusinessofDisinformationFakeNews.pdf; Steve Brozak et al., "How Martin Shkreli Used Social Media to Fuel His Short-Selling Shenanigans," STAT, July 20, 2017, https://www.statnews.com/2017/07/20/martin-shkreli-short-selling-biotech-stocks/; Renae Merle and Renae Merle, "Martin Shkreli Is Found Guilty of Three of Eight Securities Fraud Charges," *Washington Post*, August 4, 2017, https://www.washingtonpost.com/news/business/wp/2017/08/04/martin-shkreli-jury-enters-fifth-day-of-deliberations/.

[54] Brozak et al., "Martin Shkreli."

[55] Brozak et al.

SCENE 14

August 2017: White supremacists, yielding tiki torches and chanting Nazi slogans, gather at the University of Virginia the evening before a scheduled "Unite the Right" rally.[56] The group is there to protest the removal of a General Robert E. Lee statue.[57] Evidence suggests that participants on both sides had prepared for potential violence during the events.[58] Skirmishes break out between protesters and counter-protesters, resulting in at least one arrest and several minor injuries. On August 12, after the rally is prematurely dispersed by law enforcement due to increasing tensions between protesters and counter-protesters, twenty-year-old James Alex Fields, Jr., of Maumee, Ohio, deliberately drives his Dodge Challenger into counter-protesters, killing one and injuring nineteen before fleeing.[59]

Both the pre-rally events and the "Unite the Right" rally itself were primarily organized and advertised online through social media forums.[60] This resulted in tensions between groups on both sides of the political spectrum, which continue to spread online,

---

[56] The Unite the Right rally was an attempt by a number of various alt-right groups to show a unified front and protest the removal of the General Robert E. Lee confederate statue. "Charlottesville: Race and Terror – VICE News Tonight on HBO," YouTube, posted by VICE News, August 14, 2017, www.youtube.com/watch?v=P54sP0Nlngg; "Charlottesville White Nationalist Rally Blamed for 3 Deaths, Dozens of Injuries," Fox News, August 12, 2017, http://www.foxnews.com/us/2017/08/12/emergency-declared-ahead-unite-right-rally-in-virginia.html; Robert Armengol, "Three Dead, Dozens Hurt after Virginia White Nationalist Rally Is Dispersed; Trump Blames 'Many Sides,'" *Los Angeles Times*, August 12, 2017, http://www.latimes.com/nation/nationnow/la-na-charlottesville-white-nationalists-rally-20170812-story.html; Francie Diep, "How Social Media Helped Organize and Radicalize America's White Supremacists," Pacific Standard, August 15, 2017, https://psmag.com/social-justice/how-social-media-helped-organize-and-radicalize-americas-newest-white-supremacists; "'Unite The Right': Charlottesville Rally Represented Collection Of Alt-Right Groups," NPR, August 15, 2017, https://www.npr.org/2017/08/15/543730227/unite-the-right-charlottesville-rally-represented-collection-of-alt-right-groups.

[57] VICE News, "Charlottesville"; Fox News, "White Nationalist Rally Blamed for 3 Deaths"; Armengol, "Virginia White Nationalist Rally"; Diep, "Social Media and America's White Supremacists"; NPR, "Unite The Right."

[58] Nitasha Tiku et al., "Violent Alt-Right Chats Could Be Key to Charlottesville Lawsuits," *Wired*, August 27, 2017, https://www.wired.com/story/leaked-alt-right-chat-logs-are-key-to-charlottesville-lawsuits/; David Z. Morris, "Leaked Chats Show Charlottesville Marchers Were Planning for Violence," Fortune, accessed February 10, 2018, http://fortune.com/2017/08/26/charlottesville-violence-leaked-chats/; Josh Meyer et al., "FBI, Homeland Security Warn of More 'Antifa' Attacks," *POLITICO*, September 1, 2017, https://www.politico.com/story/2017/09/01/antifa-charlottesville-violence-fbi-242235.

[59] VICE News, "Charlottesville"; Fox News, "White Nationalist Rally Blamed for 3 Deaths"; Armengol, "Virginia White Nationalist Rally"; Diep, "Social Media and America's White Supremacists."

[60] Diep, "Social Media and America's White Supremacists."

garnering followers and presenting new challenges for law enforcement and first responders, especially in regards to events that could attract these opposing groups.[61] For example, on August 5, 2017, RefuseFascism.com, a website run by Bob Avakian, a 1960s radical who founded the Revolutionary Communist Party in 1975 but whose group is not affiliated with the left-wing extremist group Antifa, posted a call to action encouraging everyone to protest the Trump administration on November 4.[62] On August 30, Jordan Peltz, a little-known conservative YouTuber with no known connections to right-wing extremist groups, sits in what appears to be a law enforcement vehicle, dressed in what appears to be a law enforcement uniform. He proclaims that Antifa is preparing for an "armed uprising" on November 4.[63] This information, picked up by InfoWars, spreads throughout the internet. Concerned citizens begin to believe that a violent uprising of left-wing extremists is being planned.[64]

Meanwhile, social media users begin to post in jest about this event. One person posts, "On November 4th millions of antifa supersoldiers will stop being polite and start getting real"; another posts, "Can't wait for November 4th when millions of antifa supersoldiers will behead all white parents and small business owners in the town square."[65] Many people see these jokes online and take them seriously. More reporting by citizens, online news forums, and other platforms continues to spread this information.

---

[61] Meyer et al., "'Antifa' Attacks."

[62] "#110 The Antifa Supersoldier Spectacular," Gimlet Media, accessed December 10, 2017, https://gimletmedia.com/episode/110-antifa-supersoldier-spectacular/; Jack Smith, "The Far-Right Thinks a Violent Antifa Overthrow Is Coming Nov. 4, but the Truth Is Far Stranger," Mic Network, November 2, 2017, https://mic.com/articles/185680/the-far-right-thinks-a-violent-antifa-overthrow-is-coming-nov-4-but-the-truth-is-far-stranger.

[63] "ANTIFA Has to Go! (ORIGINAL)," YouTube video, posted by #HealTheRift, with Jordan Peltz, August 30, 2017, https://www.youtube.com/watch?v=u-klqa0FuZ4; Smith, "The Far-Right."

[64] Gimlet Media, "#110 The Antifa Supersoldier Spectacular"; Michael Edison Hayden, "'Antifa' Waging Civil War on November 4, According to Right Wing Conspiracy," *Newsweek*, October 11, 2017, http://www.newsweek.com/antifa-waging-civil-war-november-4-right-wing-conspiracy-theory-681219; Matt Christman, "On November 4th Millions of Antifa Supersoldiers Will Stop Being Polite...and Start Getting Real," Twitter, October 30, 2017, https://twitter.com/cushbomb/status/925100399622787072; Smith, "The Far-Right."

[65] Gimlet Media, "#110 The Antifa Supersoldier Spectacular"; K. T. Nelson, "Twitter Suspended Me for Trolling White Supremacists," *VICE*, October 31, 2017, https://www.vice.com/en_us/article/evbpkn/twitter-suspended-me-for-trolling-white-supremacists; Hayden, "Antifa 'Supersoldiers.'"

Further, Refuse Fascism takes out a full-page ad in the November 1 edition of the *New York Times* encouraging people to "take to the streets," because on "Nov 4. It Begins."[66] While the ad referred to "mass demonstrations," far-right media outlets and conspiracy theories continue to perpetuate the notion that Antifa is planning to violently overthrow the government.[67]

The information was so widespread that it even reached official law enforcement, public safety, and homeland security channels as a potential threat. Further, citizens who believed that Antifa was planning to overthrow the government on November 4 showed up to this protest, armed and ready to engage.[68] Protesters associated with Refuse Fascism did, in fact, show up to protest, but not to engage in the next civil war.

---

[66] Smith, "The Far-Right."

[67] Smith.

[68] Gimlet Media, "#110 The Antifa Supersoldier Spectacular."

SCENE 15

October 2017: Sixty-four-year-old Stephen Paddock, a retiree with no real criminal history or known affiliations to terrorist organizations, fires upon a crowd at a country music festival from the 32nd floor of the Mandalay Bay Resort and Casino in Las Vegas.[69] Fifty-nine people are killed and over 500 injured—the deadliest mass shooting in modern U.S. history.[70] The situation is complex: motive is not clear and the subject does not have any immediately apparent political, religious, or ideological motivations; the Islamic State immediately claims responsibility, but provides no evidence to support its claim. Nonetheless, the incident elicits a whirlwind of conspiracy theories, fake news, and falsehoods.[71] Within minutes, Twitter and other social media platforms are flooded with false information without sourcing or evidence. Some posts indicate that Paddock is an Islamic convert, or a member of the left-wing extremist group Antifa, and that the shooting was a "coordinated Muslim terror attack."[72] There are also hoaxes related to fake missing loved ones and fake photos of Paddock's "true" identity and his "true" social media pages, offering stories related to the false subject's political affiliations.[73]

---

[69] Lynh Bui et al., "At Least 59 Killed in Las Vegas Shooting Rampage, More than 500 Others Injured," *Washington Post*, October 2, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/10/02/police-shut-down-part-of-las-vegas-strip-due-to-shooting/.

[70] William Wan et al., "Las Vegas Gunman Stephen Paddock Was a High-Stakes Gambler Who 'Kept to Himself' before Massacre," *Washington Post*, October 2, 2017, https://www.washingtonpost.com/news/post-nation/wp/2017/10/02/las-vegas-gunman-liked-to-gamble-listened-to-country-music-lived-quiet-retired-life-before-massacre/; Bui et al., "Las Vegas Shooting Rampage"; "What We Know about the Las Vegas Shooting," *Washington Post*, accessed February 4, 2018, https://www.washingtonpost.com/graphics/2017/national/las-vegas-shooting/.

[71] Ryan Broderick, "Here Are All the Hoaxes Being Spread about the Las Vegas Shooting," BuzzFeed, accessed October 7, 2017, https://www.buzzfeed.com/ryanhatesthis/here-are-all-the-hoaxes-being-spread-about-the-las-vegas.

[72] Broderick.

[73] Broderick.

SCENE 16

October 2017: A website called Action News 3 reports that Morgan Freeman has passed away in his home in Charleston, Mississippi.[74] The lie spreads across Facebook and Twitter despite the fact that no credible sources reported his passing.[75]

In 2017 alone, similar lies have spread across the internet, including the hoax deaths of actor Kirk Douglas, TV personality Chumlee, musician Kid Rock, actor Andrew Lincoln, athlete Nicky Hayden, actor Clint Eastwood, musician Ted Nugent, actor Eddie Murphy, actor Rowan Atkinson, actor William H. Macy, musician Buju Banton, comedian Tommy Chong, actor Reginald VelJohnson, former President George H.W. Bush, actor Adam Sandler, and MMA fighter Ronda Rousey.[76] Many celebrities have been targets of these death hoaxes on a number of occasions spanning several years. Other individuals who are not celebrities have also become victims of this sort of activity. Ben Nimmo, a senior fellow at the Atlantic Council's Digital Forensics Research Lab, was targeted by Russian botnets after co-authoring posts online related to Russian disinformation in America, specifically writing about the use of bots.[77] The Twitter profile

---

[74] "Morgan Freeman Death Hoax," Snopes.com, October 10, 2017, https://www.snopes.com/morgan-freeman-death-hoax/.

[75] Snopes.

[76] "FACT CHECK: Ronda Rousey Death Hoax," Snopes.com, January 3, 2017, https://www.snopes.com/ronda-rousey-death-hoax/; "Adam Sandler Death Hoax," Snopes.com, January 13, 2017, https://www.snopes.com/adam-sandler-death-hoax-2/; "George H.W. Bush Death Hoax," Snopes.com, February 13, 2017, https://www.snopes.com/george-h-w-bush-death-hoax/; "FACT CHECK: Reginald VelJohnson Death Hoax," Snopes.com, February 16, 2017, https://www.snopes.com/reginald-veljohnson-death-hoax/; "Tommy Chong Death Hoax," Snopes.com, March 5, 2017, https://www.snopes.com/false-tommy-chong-dead/; "FACT CHECK: Buju Banton Death," Snopes.com, March 7, 2017, https://www.snopes.com/buju-banton-death-hoax/; "William H. Macy Death Hoax," Snopes.com, March 13, 2017, https://www.snopes.com/william-h-macy-death-hoax/; "Rowan Atkinson Death Hoax," Snopes.com, March 18, 2017, https://www.snopes.com/rowan-atkinson-death-hoax/; "Eddie Murphy Death Hoax," Snopes.com, April 24, 2017, https://www.snopes.com/eddie-murphy-death-hoax/; "Clint Eastwood Death Hoax," Snopes.com, May 15, 2017, https://www.snopes.com/clint-eastwood-death-hoax/; "FACT CHECK: Was Ted Nugent Killed in a Hunting Accident?," Snopes.com, April 28, 2017, https://www.snopes.com/ted-nugent-death-hoax/; "Nicky Hayden Death Hoax," Snopes.com, May 19, 2017, https://www.snopes.com/nicky-hayden-death-hoax/; "Andrew Lincoln Death Hoax," Snopes.com, June 17, 2017, https://www.snopes.com/andrew-lincoln-death-hoax/; "Kid Rock Death Hoax," Snopes.com, July 4, 2017, https://www.snopes.com/kid-rock-death-hoax/; "Chumlee Death Hoax," Snopes.com, July 4, 2017, https://www.snopes.com/inboxer/hoaxes/chumlee.asp; "Kirk Douglas Death Hoax," Snopes.com, December 7, 2017, https://www.snopes.com/kirk-douglas-death-hoax/.

[77] Radio Public, "IRL," 28:10.

page of one of Nimmo's colleagues was copied and then used to tweet that he had died; a Russian botnet then retweeted this information approximately 13,000 times.

While the faux killing of celebrities and other individuals may seem comical or simply a nuisance, it can disrupt the victim's life and, as is the case in Mexico, may have very deceptive undertones. A recent podcast episode by Gimlet Media, titled "The Prophet," discussed an investigation that uncovered efforts by the Mexican government to manipulate what individuals were seeing online by paying "master trolls" to amplify news that was positive toward a certain presidential candidate and burying news that was critical of that candidate.[78] When critical information went viral, the trolls were instructed to flood the internet with fake news diversions, internally dubbed a "smokescreen," often using celebrity deaths to distract from the stories they were attempting to bury.[79] These troll armies have also been reported to threaten Mexican activists' lives.[80] In fact, the reporter who uncovered this activity only did so after being sexually assaulted in a public park and using social media as a means to help her identify the attacker—a post that was quickly picked up by the internet trolls and used to harass her.[81]

---

[78] "#112 The Prophet—Reply All by Gimlet Media," Gimlet Media, accessed January 18, 2018, https://gimletmedia.com/episode/112-the-prophet/.

[79] Gimlet Media; Andalusia Knoll Soloff, "Mexico's Troll Bots Are Threatening the Lives of Activists," *Motherboard*, March 9, 2017, https://motherboard.vice.com/en_us/article/mg4b38/mexicos-troll-bots-are-threatening-the-lives-of-activists.

[80] Soloff, "Mexico's Troll Bots."

[81] Gimlet Media, "#112 The Prophet."

SCENE 17

February 2018: Nineteen-year-old Nikolas Cruz opens fire at Florida's Marjory Stoneman Douglas High School, killing seventeen and injuring fourteen.[82] Almost immediately after the shooting, student survivors start weighing in on the national gun control debate.[83] Once again, the conspiracy theory that the victims involved in the shooting are crisis actors and the shooting a false flag begin to spread rapidly online, starting with sites such as InfoWars and Gateway Pundit. The conspiracy theory soon goes viral on Facebook, Instagram, Twitter, and YouTube.[84] *Newsweek* describes what happened: "In this shadow media network, unfounded information shows up on dubious sites, churns through the news aggregation site Reddit, and works its way into Facebook feeds—and to the mainstream media."[85] Reporting by *Wired* states that these conspiracy theories were further promoted by opponents of the conspiracy who were often "outrage-sharing" the content and looking to debunk it.[86]

---

[82] "'Pure Evil': 17 Killed in Mass Shooting at Florida High School," NBC News, February 15, 2018, https://www.nbcnews.com/news/us-news/police-respond-shooting-parkland-florida-high-school-n848101.

[83] "How the Fake 'Crisis Actors' Conspiracy Took off on Social Media after Florida School Shooting," NBC News, February 22, 2018, https://www.nbcnews.com/news/us-news/how-internet-s-conspiracy-theorists-turned-parkland-students-crisis-actors-n849921.

[84] NBC News.

[85] NBC news.

[86] Molly McKew et al., "How Liberals Amped Up a Parkland Shooting Conspiracy Theory," *Wired* February 27, 2018, https://www.wired.com/story/how-liberals-amped-up-a-parkland-shooting-conspiracy-theory/.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE HITCHHIKER'S GUIDE TO ALTERNATIVE FACTS

The purpose of this research, broadly speaking, is to expose the threat posed to our national security by "fake news." This thesis answers the question: Can the information laundering model, or a modified version of the model, be used to understand how the internet is exploited to spread fake news and to explain the threat fake news poses to the nation?

I assert that a well-crafted narrative, whether true or false, can spread rapidly online due to the accessibility and interconnectedness of the internet ecosystem. I then articulate how these narratives can be disseminated even more widely, and more rapidly, when actors take advantage of existing processes that improve the customization, ease of access, and availability of information online, through both passive and active means. I do this by modifying and expanding the "information laundering" model and lexicon, which are then used to examine the interconnectedness of search engines, blogs, social networking platforms, and media/academic outlets, and how these connections can be exploited to launder false or purposefully misleading information into public discourse. Finally, I demonstrate how this process allows adversarial nations, criminals, and malicious actors to increase public discord, undermine democracy, and threaten Americans' physical and cognitive security.

A. PROBLEM STATEMENT

In its 2013 *Global Ri*sks report, the World Economic Forum warned against the global risks of massive digital disinformation and how these online risks could potentially "wreak havoc in the real world."[87] Disinformation is defined as "false, incomplete, or misleading information that is passed, fed, or confirmed to a targeted individual, group, or country."[88] The report presents two separate cases of potentially dangerous "digital

[87] "Digital Wildfires in a Hyperconnected World," World Economic Forum, accessed January 24, 2017, http://wef.ch/GJCg5E.

[88] H.R. Shultz and R. Godson, *Dezinformatsia: Active Measures in Soviet strategy* (Washington, DC: Pergamon Brassey's, 1984), 41. As quoted in Garth S. Jowett and Victoria J. O'Donnell, *Propaganda & Persuasion*, 6th Edition (Thousand Oaks, CA: SAGE, 2014), 28.

wildfires." The first is a highly tense situation in which false information is quickly spread, causing confusion, fear, and incorrect action before accurate information can be propagated. In the second situation, incorrect, though ideologically relevant, information flows within a circle of like-minded individuals who may resist attempts to correct that information.[89] The report further warns that we should "not underestimate the risk of conflicting false rumours, circulating within two online bubbles of likeminded individuals, creating an explosive situation."[90] Fast forward to the 2016 presidential election, arguably one of the most polarizing and emotional political battles of modern time, and this 2013 warning feels almost prophetic.

Citizens must now navigate an online ecosystem wherein the pathways used to find true information are the same as those used to find false information. These pathways have also been usurped by both "non-state and state actors who aim not only to disseminate misinformation but, most damaging, to erode trust in traditional sources of information."[91] This has created a political, national, and homeland security environment that often calls the very nature of truth and reality into question. What's more, outrageous conspiracy theories, once prevalent only on the fringes of society, are now being normalized and incorporated into mainstream dialogues.

When people talk about this problem, however, they typically point to social media, or even specifically to a social media platform like Facebook or Twitter, as if social media are solely responsible for the degradation of truth. In the broader sense, however, the dynamism and interactiveness of almost all websites, apps, and internet platforms, has formed a new global infrastructure for communication, sharing, and outrage. This has created an online space that, due to its complex, interconnected ecosystem, requires a new paradigm for human understanding.

---

[89] World Economic Forum, "Digital Wildfires."

[90] World Economic Forum.

[91] Bruce Wharton, "Remarks on 'Public Diplomacy in a Post-truth Society,'" in *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, ed. Shaun Powers and Markos Kounalakis (Washington, DC: United States Advisory Commission on Public Diplomacy, 2017), 7–8.

Further, a new phrase, "fake news," has become a representation of citizens' doubt, skepticism, and lack of trust, as well as a tool used by the elite to undermine facts and abuse their power. In its purest form, "fake news" refers to information meant to appear as if it is legitimate news coverage, but which is entirely or partially false. However, the term fake news has been usurped to mean any sort of bias, partisanship, mistake, or even a controversial phrase in news coverage that one simply does not agree with, often used by world leaders "to distort online discussions and suppress dissent."[92] For example, in February 2017, Syrian President Bashar Assad stated that an Amnesty International report accusing him of extensive human rights violations, including the murder of 13,000 prisoners between 2011 and 2015, was fake news.[93] In January 2018, Philippines President Rodrigo Duterte labeled a news agency that was critical of his government as fake news and said he had been unfairly demonized for his war on drugs.[94] These examples are not fake news. They are, instead, intellectual dishonesty and denialism that, if left unquestioned and unchecked, could have very real and disastrous consequences.

While fake news is certainly the zeitgeist of our time, other terms such as conspiracy theories, falsehoods, disinformation, misinformation, information warfare, and weaponized narratives have also been used. Fake news is, in fact, a very old and widely used tactic: propaganda. While the volume of and employment methods for propaganda today have evolved, understanding the fake news phenomenon through this lens offers an introductory academic framework. Further, examining how online propaganda is introduced, reinforced, and normalized via a new internet ecosystem will give policymakers, homeland security professionals, and the general public a new model through which to identify solutions that can address this problem.

---

[92] "About Us," Freedom House accessed November 19, 2017, https://freedomhouse.org/about-us; "Manipulating Social Media to Undermine Democracy: Freedom on the Net 2017," Freedom House, November 2017, https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf.

[93] Zamira Rahim, "Syria's Assad Brushes off Amnesty Report on Prison Executions as 'Fake News,'" *Time*, updated February 10, 2017, http://time.com/4666806/assad_syria-amnesty-international/.

[94] Cecilia Yap, "Duterte Decries 'Fake News' as Critics Warn of Media Crackdown," Bloomberg News, January 17, 2018, https://www.bloomberg.com/news/articles/2018-01-17/duterte-hits-fake-news-as-critics-warn-of-media-crackdown.

Anya Schiffrin, the director of technology, media, and communications specialization at Columbia University's School of International and Public Affairs, argues that people with differing opinions about how to address the internet misinformation issue are either "supply-side people" or "demand-side people."[95] Supply-side individuals believe that there is too much bad information on the internet, which makes it difficult for people to distinguish true from false information.[96] They argue that that this destructive content must be prevented before it is disseminated because, even if it is corrected, the damage (people believing the information regardless of whether or not a correction is issued) is already done. People on this side want to limit how Facebook, Twitter, and other social media platforms can circulate and promote information, and want to enforce regulations related to the money made from fake news.[97] As Schiffrin explains, demand-side individuals argue that fake news has always been around; instead of regulating it, we should seek to understand why people in today's world are more susceptible to it. People on this side argue that it is a society's responsibility to promote media literacy and critical thinking.[98]

Regardless of whether or not they are the solution, countries around the world are looking to the big technology corporations who run social media platforms to help combat mass disinformation. These social media vendors' attempts to fight against fake news have had mixed results—many argue that the attempts have been nothing more than a public relations campaign.[99] Further, Facebook and other social media vendors are continually

---

[95] Anya Schiffrin, "How Europe Fights Fake News," *Columbia Journalism Review*, October 26, 2017, https://www.cjr.org/watchdog/europe-fights-fake-news-facebook-twitter-google.php.

[96] Schiffrin.

[97] Schiffrin.

[98] Schiffrin.

[99] Barbara Ortutay, "Facebook, Google Roll out New Fact-Checking Measures," *Chicago Tribune*, April 7, 2017, http://www.chicagotribune.com/bluesky/technology/ct-facebook-google-fact-checking-fake-news-20170407-story.html; Barbara Ortutay, "Facebook Gets Serious about Fighting Fake News," AP News, December 15, 2016, https://apnews.com/22e0809d20264498bece040e85b96935/facebook-takes-fake-news; Swapna Krishna, "Facebook May Be Losing the Fight against Fake News," Engadget, November 13, 2017, https://www.engadget.com/2017/11/13/fact-checkers-say-facebook-is-losing-war-on-fake-news/.

reluctant to share user interaction data, let alone statistics related to their efforts to combat fake news, which makes it difficult to determine these efforts' effectiveness.[100]

Finally, researchers, politicians, technologists, government officials, and the general public are still sorting out the complexities of this phenomenon, making it difficult to understand all the forces at work. Although some governmental groups have signaled that this is, in fact, a homeland security issue, homeland security professionals in general have not fully recognized how fake news can impact the effectiveness and safety of emergency managers, law enforcement officers, and the public. As time goes on, this problem becomes more complex; we need a model that can adequately articulate the issue, and that can help the homeland security enterprise understand and combat its effects.

Research indicates that the disinformation problem is being tackled in an ad-hoc manner; thus far, few researchers or legislatures have addressed the phenomenon holistically by considering the totality of the internet.[101] In 2012, one researcher, Adam Klein, did recognize the potential role the totality of the internet can play in the fake news crisis, at least in regard to normalizing racist rhetoric, and it is through his foundational work that we can begin to see a framework for understanding this phenomenon. In his original model, information laundering is described as the process by 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."[102]

Taking into account the amalgamation of conspiracy theories, fake news, propaganda, and weaponized narratives spouted by extremist groups, combined with

---

[100] Krishna, "Facebook Losing against Fake News."

[101] A. J. Willingham, "Here's How to Outsmart Fake News in Your Facebook Feed," CNN, November 18, 2016, http://www.cnn.com/2016/11/18/tech/how-to-spot-fake-misleading-news-trnd/index.html; "Why the Fake News Controversy Was Really All about Facebook," Quid, accessed January 21, 2017, https://quid.com/feed/why-the-fake-news-controversy-was-really-all-about-facebook; Chengcheng Shao et al., "The Spread of Fake News by Social Bots," Cornell University Law Library, July 24, 2017, http://arxiv.org/abs/1707.07592; Daisuke Wakabayashi and Mike Isaac, "In Race against Fake News, Google and Facebook Stroll to the Starting Line," *New York Times*, January 25, 2017, https://www.nytimes.com/2017/01/25/technology/google-facebook-fake-news.html; "Silicon Valley Is Finally Realizing There's No Such Thing as 'Neutral,'" WIRED, accessed March 2, 2017, https://www.wired.com/2017/02/twitters-long-overdue-anti-abuse-tools-join-welcome-trend/.

[102] Klein, "Slipping Racism into the Mainstream," 429.

technological advancements and a growing awareness of propaganda's effectiveness, it is perhaps time to modify Klein's model. This thesis therefore proposes the Information Laundering 2.0 model.

B. RESEARCH DESIGN

Using Klein's information laundering model, which was built on theories from communication studies (specifically propaganda), I reviewed topics trending online, aspects of which were considered controversial, between January 2016 and February 2018. I attempted to identify topics from a variety of disciplines. This was especially important because the original information laundering model only considered propaganda espoused by white supremacists. Primarily, my research focused on fake news, conspiracy theories, and propaganda (often events that people witnessed unfolding in real-time) surrounding:

- White supremacist and anarchist extremist activity as well as the continued tensions between the so-called "alt-right" and "antifa."
- The 2016 presidential campaign and the first year of President Trump's administration, including suspected influence operations by the Russian government and the spreading of fake news by Macedonians.
- Critical incidents, specifically the Pulse Nightclub shooting in Orlando in 2016, the Las Vegas shooting in 2017, the Sutherland Springs shooting in 2017, and the Parkland, Florida, school shooting in 2018.
- Natural disasters, specifically Hurricane Matthew in 2016, Hurricane Harvey in 2017, and Hurricane Maria in 2017.

Original source material, as well as secondary sources related to the events (both scholarly and media reporting), were reviewed. Using Jowett and O'Donnell's ten divisions for propaganda analysis, I reviewed potential propaganda surrounding each incident and sought to identify "the ideology and purpose of the propaganda campaign," "the context in which the propaganda occurs," "identification of the propagandist," "the structure of the propaganda organization," "the target audience," "media utilization techniques," "special

techniques to maximize effect," "audience reaction to various techniques," "counterpropaganda, if present," and "effects and evaluation."[103] Looking for "cultural myths and stereotypes" reinforced by propaganda messaging, I then traced the flow of this content through various online platforms to attempt to validate the categories described in the original information laundering model (search engines, blogs, social media, and news and research), noting areas where additional tools or processes were being leveraged to maximize effect. Additionally, I reviewed each communication to discern strategies and techniques that impacted a reader's inherent cognitive biases, especially things like implicit egotism, the false consensus effect, and the availability heuristic. I also reviewed the layout of the source content and website itself to identify if there were aspects of that layout that made that content seem more credible (technical-ethos). These datasets and research were applied to the information laundering framework, which ultimately led me to modify the model to better explain the existing internet ecosystem's impact on propaganda.

It should be noted that the significance of this research also lends to its limitations. As Jowett and O'Donnell explain, it can be difficult to discuss propaganda analysis in real-time through this framework; however, doing so "enables the analyst to observe media utilization and audience response directly in actual settings."[104] While this research is therefore relevant and timely, scholarly journals and academic studies were not always available for propaganda analysis. Nonetheless, because the internet ecosystem evolves quickly, it was crucial that the research relied on the most current examples. Existing and emerging technologies were considered when determining the information laundering model's feasibility within our current situation. Of course, academic and official research were used whenever possible to validate the existing and emerging technological impact on online propaganda.

Ultimately, this research demonstrates how the interconnectedness of various internet platforms, coupled with existing and emerging online technologies, can be exploited to launder false or purposefully misleading information into public discourse at

---

[103] Jowett and O'Donnell, *Propaganda & Persuasion*, 313.

[104] Jowett and O'Donnell, 313.

a volume and velocity previously unimaginable. This research is important because this ongoing threat continues to raise difficult discussions among homeland security professionals, policymakers, and the general public, often creating an uncomfortable dialogue in which partisanship, freedom of speech, and privacy laws come into play. Nonetheless, establishing a practical framework, the Information Laundering 2.0 model, to help explain this phenomenon is a crucial step toward effective and sustainable actions to combat it.

II. THE WAR (OF WORDS) TO END ALL WARS

The spread of disinformation is not a new phenomenon. This tactic was used by the Catholic Church to undermine the Emperor Constantine, by adversaries of the Knights Templar to manipulate the Knights to surrender, and by Benjamin Franklin to prove the power and impact of words.[105] Historically, however, these cases had little impact on most people's daily lives. The literature review that follows examines how content-sharing methods can undermine the credibility of legitimate sources by leveling the playing field for false or extremely biased sources, masquerading as credible sources, to enter the public debate. Further, a new concept called counterfeit narratives is proposed; this concept seeks to integrate the breadth of propaganda tactics into the information age.

A. CONSPIRACY THEORIES

A conspiracy theory is best defined as "the belief that an organization made up of individuals or groups was or is acting covertly to achieve some malevolent end."[106] However, like many other areas of social science research, locking down a standard definition of a conspiracy theory can be difficult. More importantly, it is critical to discuss the research surrounding conspiracy theories in order to understand why conspiracy theories, and people who believe in conspiracy theories, seem to be on the rise.

Although there was little research dedicated to the study of conspiracy theories until recently, today there are typically two schools of thought on why conspiracy theories form and proliferate.[107] The first is referred to as an "individualistic" framework and pioneered

---

[105] Krystal D'Costa, "Three Historical Examples of 'Fake News,'" Scientific American Blog Network, accessed August 20, 2017, https://blogs.scientificamerican.com/anthropology-in-practice/three-historical-examples-of-fake-news/; "Fake News? That's a Very Old Story," *Washington Post*, November 25, 2016, https://www.washingtonpost.com/opinions/fake-news-thats-a-very-old-story/2016/11/25/c8b1f3d4-b330-11e6-8616-52b15787add0_story.html.

[106] Michael Barkun, *A Culture of Conspiracy: Apocalyptic Visions in Contemporary America (Comparative Studies in Religion and Society)*, 2nd edition (Berkeley: University of California Press, 2013), 3, https://www.amazon.com/dp/B00DNJD46C/ref=docs-os-doi_0.

[107] Adam Conover, "Dr. Daniel Jolley on Why Conspiracy Theories Are Harmful," *Adam Ruins Everything* (podcast), January 24, 2018, http://www.maximumfun.org/adam-ruins-everything/adam-ruins-everything-episode-44-professor-daniel-jolley-why-conspiracy-theori.

by Richard Hofstadter, a professor of American history at Columbia University, and many others.[108] It surmises that those who participate in conspiracy theories have a paranoid personality type; they tend to use others as scapegoats and have an "us versus them" worldview. Individualistic framework scholars argue that conspiratorial thinking is linked to more marginalized groups because they feel powerless. Tabloid magazines and other unreliable sources of information help grow the conspiratorial beliefs, and exposure to legitimate or fact-based sources does little to change conspiracy theorists' minds.[109]

The second school of thought, championed, among others, by Peter Knight, a professor of English and American studies at the University of Manchester, can be viewed more from a "cultural sociology" lens. Like the "paranoid" school of thought, marginalized individuals who consume more "non-mainstream material" are more likely to proliferate conspiracy theories, but cultural sociology, such as the "pervasiveness of government secrecy," plays a much larger role.[110] Conspiracy theories often persist because they are viewed as "entirely plausible"—they raise awareness about "behind the scenes" information, increasing cynicism toward corporate and government power.[111] This second block of theories is important because

> from the cultural sociological perspective, conspiracy theorizing appears *less* as psychological short-circuiting that further marginalizes already disempowered groups and *more* a form of populist protest against powerful elites, often by politically engaged members of outsider groups.[112]

In his book *A Culture of Curiosity*, Michael Barkun, professor emeritus of political science at Syracuse University, discusses the "conspiracist subculture that has become more visible since September 11, 2001."[113] He explains how these subcultures weave

---

[108] Carl Stempel, Thomas Hargrove, and Guido H. Stempel III, "Media Use, Social Structure, and Belief in 9/11 Conspiracy Theories," *Journalism and Mass Communication Quarterly* 84, no. 2 (2007): 354–355.

[109] Stempel, Hargrove, and Stempel, 354–355.

[110] Stempel, Hargrove, and Stempel, 355.

[111] Stempel, Hargrove, and Stempel, 355–356.

[112] Stempel, Hargrove, and Stempel, 356.

[113] Barkun, *A Culture of Conspiracy*, 1.

together unorthodox beliefs, occult-like ideas, radical politics, and fringe science, usually emerging during a crisis and sometimes with great influence on society.[114] Barkun identifies three underlying principles of all conspiracy theories: "nothing happens by accident," "nothing is as it seems," and "[everything] is connected."[115] These principles create conspiracy theories that reside in closed-off, self-fulfilling loops that soon become "nonfalsifiable, because every attempt at falsification is dismissed as a ruse."[116] Barkun attributes the rise of conspiracy theories today to "stigmatized knowledge": claims that conspiracy theorists insist are true, but that have not been validated by mainstream entities. These theories find a comfortable niche on the internet, where they can reach like-minded individuals.[117]

Given this rise in conspiracy theories today, it is important to understand not only the individual factors, but also the sociological and technological factors that may be impacting their proliferation. It is important to note that conspiracy theories, unlike "fake news," do not necessarily represent a nefarious attempt to push disinformation. Conspiracy theory purveyors often believe the information they are disseminating is accurate, and present what they believe is empirical evidence to validate their claims.[118]

Daniel Jolley, a professor of psychology who studies conspiracy theories at Staffordshire University in the United Kingdom, explains that conspiracy theories often develop from our normal tendency to imagine that "big events must be explained by something equally big."[119] When big events happen, according to Jolley, people feel powerless, out of control, anxious, and uncertain, especially when the true cause of events is unknown. A conspiracy theory, then, may act as a coping mechanism for someone's anxious initial reactions, offering a quick path to control and certainty.[120]

---

[114] Barkun, 2.

[115] Barkun, 3.

[116] Barkun, 7.

[117] Barkun, 12–13.

[118] Barkun, 6.

[119] Conover, "Dr. Daniel Jolley on Why Conspiracy Theories Are Harmful."

[120] Conover.

The effects of this coping mechanism, however, may be temporary. Current research suggests that as people continue to be exposed to conspiracy theories, they actually tend to feel more uncertain, distrustful, and powerless in the long run.[121] While more research is still needed in this realm, conspiracy theories come with potential harmful consequences. Jolley and Douglas's research suggests that people who are exposed to conspiracy theories can lose trust and become inactive.[122] For example, they found that if people are presented with information that suggests climate change is a hoax or vaccinations are unsafe, they are less likely to take steps to reduce their carbon footprint or to have their children vaccinated.[123] So, while it is important to think critically—to ask questions and challenge the mainstream narrative, when appropriate—people must strike a balance between believing everything and believing nothing. Nonetheless, when establishing a framework for combatting the spread of misinformation, conspiracy theories, though a part of the puzzle, do not adequately capture the breadth of falsehoods being promulgated online, nor do they necessarily elicit the need for individuals, society, the government, or the globe to actively fight back against it.

B. FAKE NEWS

Another form of misinformation, "fake news" is a familiar term to most. In its simplest definition, it is "hoax-based stories that perpetuate hearsay, rumors, and misinformation."[124] Freedom House refers to fake news as "intentionally false information that has been engineered to resemble legitimate news and garner maximum attention."[125] This definition clarifies that fake news is not only intentionally produced, but also

---

[121] Conover.

[122] Conover; Daniel Jolley and Karen M. Douglas, "The Social Consequences of Conspiracism: Exposure to Conspiracy Theories Decreases Intentions to Engage in Politics and to Reduce One's Carbon Footprint," *British Journal of Psychology* 105, no. 1 (February 2014): 35–56, https://doi.org/10.1111/bjop.12018; Jolley and Douglas, "Anti-vaccine Conspiracy Theories."

[123] Jolley and Douglas, "Social Consequences of Conspiracism"; Jolley and Douglas, "Anti-vaccine Conspiracy Theories."

[124] 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, http://journals.sagepub.com/doi/abs/10.1177/0002764217701217.

[125] Freedom House, "Manipulating Social Media," 12.

engineered to elicit great attention. This is an important observation; fake news that nobody sees, cares about, or believes will not achieve the virality and impact intended by its propagators. American PEN, the U.S.-based center for PEN International, which aims to "defend free expression, support persecuted writers, and promote literary culture" describes fakes news as "demonstrably false information that is being presented as a factual news report with the intention to deceive the public."[126] In this definition, the intent of the fake news, "to deceive the public," is explicitly noted.

However, the term fake news itself has taken on a number of meanings. Digital Shadows, a digital risk-management firm, probably described it best, stating, "Fake news is used very broadly to describe: disinformation, propaganda, hoaxes, satire and parody, inaccuracies in journalism, and partisanship."[127] Although fake news does represent the zeitgeist involving disinformation campaigns, it does not capture the full breadth of the disinformation phenomenon. Because the term has been politicized so egregiously, it has become almost meaningless. In fact, a 2018 study at MIT on the spread of true and false news online asserted, "The term has lost all connection to the actual veracity of the information presented, rendering it meaningless for use in academic classification."[128] Instead, we must look to a much older term—a concept that has been described by scholars for centuries. Propaganda.

C. PROPAGANDA

Both conspiracy theories and fake news have been used as tools in larger disinformation, or propaganda, campaigns. In terms of the current threat facing our society, it is propaganda—along with its virality and speed—that is most important. Traditional propaganda has been described by historians, journalists, political scientists, sociologists, psychologists, and philosophers, and a large body of research exists on this subject.[129] It

---

[126] PEN America, F*aking News: Fraudulent News and the Fight for Truth* (New York: PEN America, 2017), 23, https://pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf.

[127] Digital Shadows, "The Business of Disinformation."

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

[129] Jowett and O'Donnell, *Propaganda & Persuasion*, 1.

is common today to use the word "propaganda" as if there were a single, agreed-upon meaning. And although the majority of scholars agree that propaganda is effective when its purpose is persuasive, they lack consensus when it comes to what can or should be considered propaganda. Scholars tend to disagree most frequently over three key aspects: the scope of the propaganda, whether propaganda should be viewed as malicious or neutral, and who should be considered a propagandist. These factors, all of which are discussed in this section, are often considered interdependently.

Until World War II, the term propaganda had fewer negative connotations; it was viewed as efforts to promote. Edward Bernays, often considered the father of public relations, viewed propaganda as a way for a few individuals to manipulate the masses in an effort to push social and political agendas.[130] Bernays's view on propaganda was neutral. He saw it as a useful tool employed by the intelligent minority to help the "public at large become aware of and act upon new ideas."[131] To Bernays, propaganda is a public relations function, and both governments and corporations must consult public relations advocates if they want to use it effectively.[132] Thus, Bernays considers corporations as propagandists, and considers corporate propaganda within the scope of propaganda in general. In fact, many argue that Bernays was spouting "propaganda for propaganda," attempting to appeal to potential corporate clients who might benefit from his expertise.[133]

Jacques Ellul, a French philosopher and sociologist, saw propaganda as the result of biased men and biased messages in a technological society.[134] To Ellul, propaganda is a "sociological phenomena, not … something made or produced by people of intentions."[135] In his view, any message with an intentional or unintentional bias is propaganda. Ellul asserts that propaganda is everywhere and in everything, which makes

---

[130] Edward Bernays, *Propaganda*, Kindle edition (New York: Ig Publishing, 2004).

[131] Bernays, 58.

[132] Bernays, 65.

[133] Bernays, 17.

[134] Jacques Ellul, *Propaganda: The Formation of Men's Attitudes*, trans. Konrad Kellen and Jean Lerner (New York: Vintage, 1973), https://www.amazon.com/Propaganda-Formation-Attitudes-Jacques-Ellul/dp/0394718747/ref=sr_1_3?ie=UTF8&qid=1512952599&sr=8-3&keywords=jacques+ellul.

[135] Jowett and O'Donnell, *Propaganda & Persuasion*, 3.

it difficult to systematically study. Nonetheless, many scholars agree with Ellul. Leonard Doob, a psychology professor at Yale University from 1935 to 1999, actually refused to define propaganda, arguing that it means different things in different societies or in different times.[136]

From this perspective—if propaganda is a force outside of our control that is not necessarily promulgated by a specific actor or actors—homeland security professionals need not trouble themselves about propaganda, since they play no role in combating this kind of force. However, when looking at Russia's recent interference in the U.S. elections or the conspiracy theories leading to armed conflict and violence, there do appear to be human actors at work; thus if one wants to identify, quantify, and analyze propaganda, both Ellul and Doob leave something to be desired.

Alex Carey, a lecturer in psychology and industrial relations at the University of New South Wales and author of *Taking the Risk out of Democracy: Corporate Propaganda versus Freedom and Liberty*, emphasized the role that corporations and big businesses play in the spread of propaganda.[137] He introduces the concept of "domestic propaganda"; rather than being directed outwards to try to undermine or deflect a foe during wartime, domestic propaganda is directed inwards onto the electorate to further the "the interests of privileged segments of that society."[138] Carey argues that corporate propaganda, especially when employed through commercial advertising and public relations, is the most common form of propaganda activity in a democracy.[139] He posits that, in the twentieth century, three important political developments occurred: "the growth of democracy, the growth of corporate power, and the growth of corporate propaganda as a means of protecting

---

[136] Jowett and O'Donnell, 4.

[137] Jowett and O'Donnell, 6.

[138] Alex Carey, *Taking the Risk Out of Democracy: Corporate Propaganda versus Freedom and Liberty (History of Communication)*, 1st edition (Champaign: University of Illinois Press, 1996), 11, https://www.amazon.com/Taking-Risk-Out-Democracy-Communication/dp/0252066162/ref=sr_1_1?s=books&ie=UTF8&qid=1512963129&sr=1-1&keywords=taking+the+risk+out+of+democracy.

[139] Jowett and O'Donnell, *Propaganda & Persuasion*, 5; Carey, *Taking the Risk Out of Democracy*, 14.

corporate power against democracy."[140] Further, he concludes that corporate propaganda's ability to convince consumers that they are free from propaganda "is one of the most significant propaganda achievements of the twentieth century."[141] While consumers are perhaps more skeptical about big business today than in the past, these observations are certainly still relevant and important. Through his work on corporate propaganda, Carey expands the concepts of who can be considered a propagandist and what can be considered a motive for propaganda. In this case, capitalists who have a financial motivation employ propaganda to enhance their brand and sell more products.

Later, Edward Herman and Noam Chomsky took this one step further, publishing *Manufacturing Consent: The Political Economy of the Mass Media.*[142] In this book, the authors discuss the role of mass media, specifically that "it is their function to amuse, entertain, and inform, and to inculcate individuals with the values, beliefs, and codes of behavior that will integrate them into the institutional structures of the larger society."[143] They argue that the government and major corporations use the mass media to help inform and educate the general population on its ideals. The mass media therefore reinforces the status quo, supporting the ruling economic and political classes that in essence control society.[144] Before press coverage occurs, they explain, it must be passed through several filters, meaning the news that is actually reported is heavily in favor of those in power.

These concepts have massive implications for the disinformation phenomenon today, especially considering our almost unlimited access to information online. In the current media environment, mass media (today referred to as mainstream media) are no longer the gatekeeper of information. Further, the idea that the government and corporations use mass media to retain power offers a starting point for not only civil rights

---

[140] Carey, *Taking the Risk Out of Democracy*, 18.

[141] Carey, 21.

[142] Edward S. Herman and Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*, Kindle edition (New York: Pantheon, 2011), https://www.amazon.com/Manufacturing-Consent-Political-Economy-Media-ebook/dp/B0055PJ4R0/ref=sr_1_1?ie=UTF8&qid=1514414505&sr=8-1&keywords=manufacturing+consent+noam+chomsky.

[143] Herman and Chomsky, sec. 1341.

[144] Herman and Chomsky.

and other activists who are looking to effect positive change, but for conspiracy theorists and foreign nations who wish to undermine democracy.

In 2001, psychologists Anthony Pratkanis and Elliot Aronson proposed that propaganda is everywhere and that it is, in essence, the abuse or perversion of persuasion.[145] To Pratkanis and Aronson, rather that providing us with straightforward facts and information to help make an informed decision, propaganda works to catch us off guard so we can be influenced without our knowledge. Propaganda is accomplished through positive language, and by the speaker framing the argument in a way that causes the individual to focus on the feelings of pleasure, rather than facts.[146] Pratkanis and Aronson offer four stratagems of propaganda influence: source credibility (have the message delivered by a trusted or admired source), messaging (use positive affirmations to frame the message in a positive light), pre-persuasion (create a vulnerable mindset), and emotions (cater the message to the target's emotional response).[147] This concept is important when considering the ecosystem of the internet and online propaganda. In a world full of distractions, it becomes more difficult for the busy consumer or distracted citizen to make informed decisions based on facts.

Garth S. Jowett, a professor of communications at the University of Houston, and Victoria O'Donnell, a professor of communications at Montana State University–Bozeman, have written six editions of *Propaganda & Persuasion*, which includes a comprehensive history of propaganda as well as ways to analyze and understand it in the modern age.[148] In their view, propaganda combines deliberate intent with a systematic plan to achieve its purpose, a process that distinguishes propaganda from "a free and open exchange of ideas."[149] Jowett and O'Donnell acknowledge that propaganda has been used

---

[145] Anthony Pratkanis and Elliot Aronson, *Age of Propaganda: The Everyday Use and Abuse of Persuasion* (New York: Holt Paperbacks, 2001), https://www.amazon.com/Age-Propaganda-Everyday-Abuse-Persuasion/dp/0805074031/ref=sr_1_1?ie=UTF8&qid=1512962691&sr=8-1&keywords=pratkanis+and+aronson.

[146] Pratkanis and Aronson.

[147] Pratkanis and Aronson.

[148] Jowett and O'Donnell, *Propaganda & Persuasion*, 19.

[149] Jowett and O'Donnell, 19.

by a variety groups, organizations, and ruling parties across the political, economic, and social spectrum. Whether it is a government entity looking to instill a message in its citizens, a terrorist organization attempting to recruit followers, or a company trying to convince customers to purchase its merchandise over a competitor's, the objective is to "reinforce or modify the attitudes, the behavior, or both of an audience."[150]

Jowett and O'Donnell acknowledge that an individual's perception of communication determines if the communication is considered "self-evident" or "controversial."[151] "One person's propaganda," they say, "may be another person's education."[152] However, by viewing propaganda through a communications lens, it can be defined as deliberate attempts to manipulate an audience through a systematic plan that results, or attempts to result, in an outcome that is advantageous to the propagandist; this is what differentiates propaganda from a free and open exchange of ideas (see Figure 1).[153]

[150] Jowett and O'Donnell, 4.

[151] Jowett and O'Donnell, 19.

[152] Jowett and O'Donnell, 20.

[153] Jowett and O'Donnell, 19.

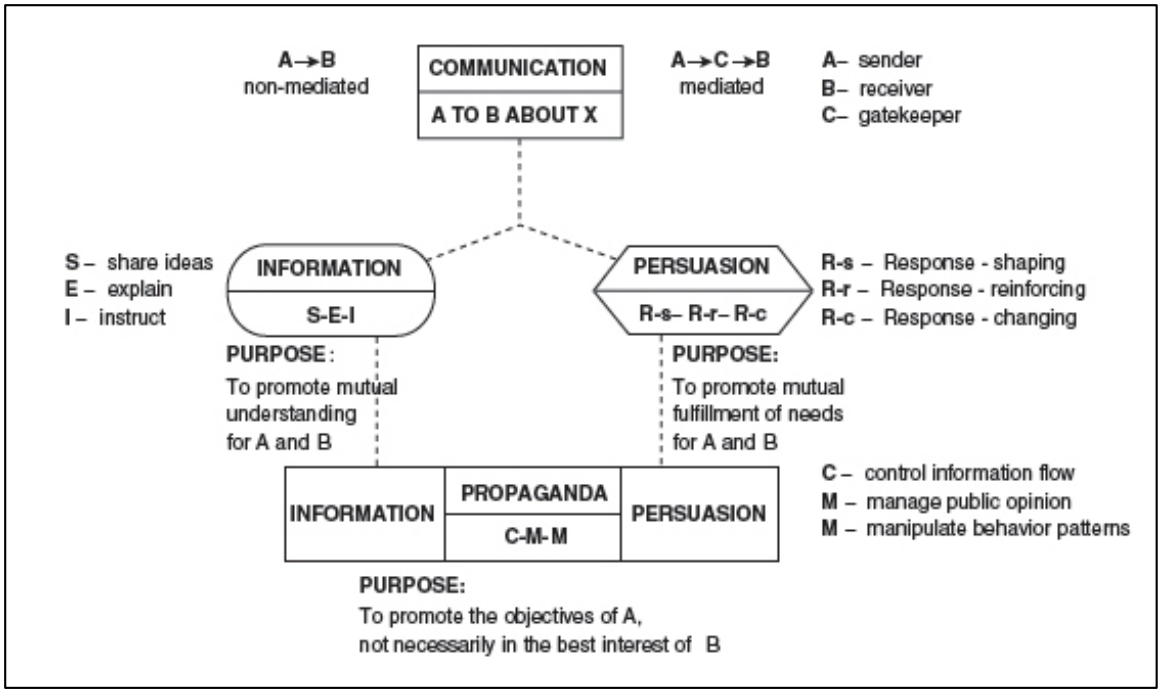

Figure 1. The Jowett and O'Donnell Purpose Model of Propaganda[154]

This viewpoint can help establish a systematic framework and a model to analyze a process without value judgement.[155] Therefore, for purposes of this thesis, I use the definition of propaganda proposed by Jowett and O'Donnell: "Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist."[156]

Because not all propaganda is created equal, Jowett and O'Donnell also provide definitions for various forms of propaganda—a sort of propaganda spectrum. They break propaganda primarily into three categories: white propaganda, black propaganda, and gray propaganda. White propaganda is neither deceitful nor false.[157] The recipient is aware of the source of the propaganda and the message it intends to relay, including the perspective the purveyor is taking. For example, a public health agency may leverage white propaganda

[154] Source: Jowett and O'Donnell, 34.

[155] Jowett and O'Donnell, 1.

[156] Jowett and O'Donnell, 6.

[157] Jowett and O'Donnell, 20.

to inform the public about an influenza outbreak and encourage people to get flu shots. White propaganda is often referred to as "spin" or "news management."[158] Bernays therefore would have been a professional white propagandist.

Black propaganda conceals or discredits the source of the information and "spreads lies, fabrications, and deceptions."[159] The term disinformation is also consistent with black propaganda because it is intentionally false and sourced covertly.[160] Here, Jowett and O'Donnell discuss a history of completely fabricated documents, such as *The Protocols of the Elders of Zion*, meant to arouse antisemitism. They also describe uses of black propaganda in war time such as "The Ghost Army," which intended to trick World War II Germans into believing that Allied Forces were scattered all over Europe. American men arrived in France with audiovisual sound effects and equipment to mimic the sounds of battle, and trick the Germans into planning for battle or opening fire on false armies.[161] In another example, the British inserted their own material into American press so they could then quote this material during radio broadcasts. Jowett and O'Donnell explain, "The success or failure of black propaganda depends on the receiver's willingness to accept the credibility of the source and the content of the message."[162] There is therefore a burden on the propagandist to understand the message's context—if the propagandist does not have sufficient cultural, social, and political awareness to relay a message that is believable, the black propaganda is likely to fail.[163]

Somewhere between white and black propaganda is gray propaganda. With gray propaganda, "the source may or may not be correctly identified, and the accuracy of the information is uncertain."[164] According to Jowett and O'Donnell, gray propaganda is often used to embarrass another party. For example, after the assassinations of Martin Luther

---

[158] Jowett and O'Donnell, 3.

[159] Jowett and O'Donnell, 20.

[160] Jowett and O'Donnell, 26.

[161] Jowett and O'Donnell, 22.

[162] Jowett and O'Donnell, 23.

[163] Jowett and O'Donnell, 23.

[164] Jowett and O'Donnell, 25.

King, Jr., and President John F. Kennedy, Radio Moscow took advantage of the events to denigrate the United States; when Edward Snowden leaked classified documents, China sought to embarrass the United States by hailing Snowden as a hero in its state-run media.[165] The United States has also engaged in gray propaganda efforts, Jowett and O'Donnell explain, often planting favorable articles in foreign media. Corporations and private businesses engage in gray propaganda as well, providing media clips for potential inclusion in news television broadcasts and online media.

Jowett and O'Donnell also discuss "subpropaganda" or "facilitative communication," which is the propagandist's attempt to prime an audience to accept a specific belief or doctrine that is currently unfamiliar or unaccepted. It is also a means for a target to develop a favorable or positive attitude toward a potential propagandist, priming them for future messaging.[166] Other techniques that can enhance a propagandist's efforts have also been noted. Pratkanis and Aronson describe the "granfalloon technique," which involves grouping some people together while excluding others to create a sense of camaraderie at the expense and isolation of others. Another technique, "mass criticism," involves continuous attacks on the credibility of messages, even if the messages are true and accurate, which can increase a person's doubt about the information.[167] The more doubt a person feels about a piece of information, the less likely he or she will be to act on the information.[168]

With Jowett and O'Donnell's definition of propaganda in mind, it can be argued that organized efforts to spread false online are really just an evolution of propaganda tactics. Nonetheless, because these campaigns can now quickly go viral, there is a greater chance that more people will believe them, which makes our ability to combat disinformation all the more challenging. As a result, simply referring to this phenomenon

---

[165] Jowett and O'Donnell, 25.

[166] Jowett and O'Donnell, 31.

[167] Matt Chessen, "Understanding the Psychology Behind Computational Propaganda," in *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, ed. Shaun Powers and Markos Kounalakis (Washington, DC: United States Advisory Commission on Public Diplomacy, 2017), 21.

[168] Chessen, 21.

as propaganda also does not recognize this bigger threat. To help understand the issue on a proper scale, we must consider weaponized and counterfeit narratives.

D. WEAPONIZED NARRATIVES AND COUNTERFEIT NARRATIVES

In an attempt to define the propaganda of the information age, a new term, "weaponized narrative," has emerged. Weaponized narratives, grounded in the concept of hybrid warfare, are developed by an adversary to "deploy in a rapid-fire series of mutually-reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal cost."[169] The Center on the Future of War, a partnership between Arizona State University and the independent think tank New America, suggests that weaponized narratives are the "new battlespace" of war.[170] The premise centers around "destroying an enemy's intent or *will* to threaten."[171] Weaponized narratives, unlike natural ones, are designed for speed of transmission, virulence, and exploitation of vulnerabilities in the mind to destroy the will.[172] No longer is war only about lethality; it is also about legitimacy.[173]

According to Jon Hermann, weaponized narratives are identified based on their "Vector, Vulnerability, and Virulence; Scope, Speed, and Synergy."[174] *Vector* refers to a delivery system's impact on a particular item's reach or prominence. A well-crafted narrative could have global reach given that its vector, information, is self-propagating.

---

[169] "A form of warfare in which one of the combatants bases its optimized force structure on the combination of all available resources—both conventional and unconventional—in a unique culture context to produce specific, synergistic effects against a conventionally-based opponent." Timothy B. McCulloh and Richard B. Johnson, *Hybrid Warfare*, JSOU Report 13-4 (MacDill AFB, FL: JSOU, 2013), 17; Jon Herrmann, "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War," *The Strategy Bridge*, July 27, 2017, https://thestrategybridge.org/the-bridge/2017/7/27/nine-links-in-the-chain-the-weaponized-narrative-sun-tzu-and-the-essence-of-war.

[170] Brad Allenby and Joel Garreau, "Weaponized Narrative: The New Battlespace" (white paper, The Center on the Future of War, 2017), http://azhumanities.org/wp-content/uploads/2017/08/WN-weaponized-narrative_final_compressed.pdf.

[171] Herrmann, "Nine Links in the Chain."

[172] Herrmann.

[173] Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Santa Barbara, CA: Praeger, 2009), 207, https://www.amazon.com/War-2-0-Irregular-Information-International/dp/0313364702/ref=sr_1_2?ie=UTF8&qid=1510502399&sr=8-2&keywords=war+2.0.

[174] Herrmann, "Nine Links in the Chain."

Vulnerability refers to how susceptible something is to attack or harm.[175] Given cognitive factors (outlined in the next section), a well-crafted narrative could exploit vulnerabilities in the human mind. *Virulence* refers to how likely something is to exploit a vulnerability on a massive scale.[176] A well-crafted narrative that exploits our cognitive biases certainly has the potential for virality. *Scope*, per Hermann, refers to the number of people who could be actors in a particular threat space. Because the internet facilitates easy, low-cost information flow, there is a potentially limitless scope of actors to create well-crafted narratives. *Speed* refers to how quickly information could be propagated and then reinforced.[177] Given the tools available to actors through technology (outlined in Chapter III), a well-crafted narrative could be reinforced almost instantaneously. *Synergy* refers to how each aspect of a system is a force-multiplier to all other parts of the system.[178]

It is further important to note that weaponized narratives, such as those employed by Russia in the United States and Europe, are of major concern; domestically, however, many governments use weaponized narratives to maintain or consolidate power. In fact, a well-crafted narrative is easily laundered through the internet ecosystem with a force-multiplying effect (outlined in Chapter IV). In 2017, Freedom House identified thirty countries (including Venezuela, the Philippines, and Turkey) in which the government employed "armies of 'opinion shapers' to spread government views, drive particular agendas, and counter government critics on social media."[179] According to Freedom House: "Authoritarians have effectively taken up the same tools that many grassroots democratic activists used to disrupt the state media narrative, and repurposed them to advance an antidemocratic agenda."[180]

---

175 Herrmann.

176 Herrmann.

177 Herrmann.

178 Herrmann.

179 Freedom House, "Manipulating Social Media."

180 Freedom House, 8.

While the term "weaponized narratives" certainly evokes the danger and harm these activities elicit, it draws people's attention away from other actors who may employ similar strategies. Therefore, I propose a new term, "counterfeit narrative," which more accurately accounts for all of the potential actors who could leverage these tools, including nation-states, terrorist organizations, domestic extremists, and even corporations that engage in disingenuous advertising campaigns. A counterfeit narrative is therefore online content, or a series of content, created for the purposes of information laundering. The content of a counterfeit narrative benefits the propagandist and has a negative or destructive effect on its recipient. More so than terms like fake news, conspiracy theory, weaponized narrative, and even propaganda itself, the term counterfeit narrative more effectively captures the nuances of the disinformation, the actors disseminating it, and the spreadability of that propaganda online.

E. ETHOS, PATHOS, LOGOS, AND THE EFFECTIVENESS OF COUNTERFEIT NARRATIVES

For a counterfeit narrative to be effective, it must be persuasive. Aristotle wrote about persuasion in 350 BCE, offering that a spoken or written communication is most persuasive when it appeals to authority (*ethos*), emotion (*pathos*), and logic (*logos*).[181] Authority, or ethos, in many cases is established by the source's, or speaker's credibility. Many factors can lend perceived credibility to a source, including the variety of sources it incorporates; the number, volume, and variety of endorsements; and the authority of other individuals who promote and endorse those sources.[182] If several sources or individuals make contrasting arguments that ultimately lead to the same conclusion, the message they are relaying becomes more persuasive than if that same conclusion were to come from a single source.[183] Additionally, if a large number of different individuals endorse the message, regardless of whether or not those subjects themselves are individually credible,

[181] Aristotle, *On Rhetoric: A Theory of Civic Discourse, 2nd Edition*, trans. George A. Kennedy, 2nd edition (Oxford: Oxford University Press, 2006), https://www.amazon.com/Rhetoric-Theory-Civic-Discourse-2nd/dp/0195305094/ref=dp_ob_title_bk.

[182] Chessen, "Computational Propaganda."

[183] Chessen.

the message may appear more persuasive.[184] Finally, if other sources have been determined to be credible, and these sources also relay the message, the content will be considered more credible.[185]

Whether it be from a country, a political party, or a group of consumers, the goal of a counterfeit narrative is to influence and persuade a large number of people. In fact, much of the literature on propaganda refers to the phenomenon as "mass persuasion."[186] Gustave Le Bon, a French psychologist, refers to a collective mass vulnerable to propaganda as a "crowd," which he defines as "a gathering of individuals of whatever nationality, profession, or sex, and whatever by the chances that have brought them together."[187]

Le Bon was one of the first scholars to write about crowds' susceptibility to propaganda, and this phenomenon's potential to negatively impact civilizations. In his 1895 book, *The Crowd: A Study of the Popular Mind*, Le Bon argues that a leader can persuade a crowd through affirmation, repetition, and contagion.[188] Le Bon has a clear animosity toward crowds, arguing that, as individuals form a crowd, they lose their individual rationality and dissolve into a single, simplified group mentality, which can be easily used, influenced, manipulated, and abused by powerful leaders.[189] To Le Bon, propaganda is a natural phenomenon that occurs within a crowd, and one that should be closely monitored; he argues: "Civilisations as yet have only been created and directed by a small intellectual aristocracy, never by crowds. Crowds are only powerful for destruction."[190]

---

[184] Chessen, 20.

[185] Chessen, 21.

[186] Jowett and O'Donnell, *Propaganda & Persuasion*, 33.

[187] Gustave Le Bon, *The Crowd: A Study of the Popular Mind*, Kindle edition (Overland Park, KS: Digireads, 2004), 18, https://www.amazon.com/Crowd-Study-Popular-Mind-ebook/dp/B000FC230S/ref=pd_sim_351_7?_encoding=UTF8&psc=1&refRID=Z96WDJYACZVPEA5D667Y.

[188] Le Bon, 124.

[189] Le Bon.

[190] Le Bon, 11.

On the other hand, in 2005, James Surowiecki (in his well-known book, *The Wisdom of Crowds*), takes the opposite view in relation to crowds. Whereas Le Bon looks at a crowd and sees homogeneity and madness, Surowiecki believes that the larger a crowd, the more intelligent it can be. Surowiecki argues that the knowledge generated by a decentralized, heterogeneous crowd that can maintain independent thinking and whose judgements can be properly aggregated will be superior to knowledge generated by an individual or even a group of experts.[191] Surowiecki acknowledges that herd mentality and groupthink, as discussed by Le Bon, continue to pose a risk to proper collective intelligence, but that this can be overcome by maintaining the proper characteristics of the intelligent crowd.[192] Surowiecki argues that individual group members must maintain their ability to think independently, and maintain their own sources of information.[193] The group must be sufficiently diverse, to allow for a range of ideas and opinions, and crowds are most successful when decentralized, rather than when controlled by a single leader.[194] However, the individual pieces of the decentralized group must be collected and assessed in a central location to prevent them from missing the larger picture.[195]

Neither Le Bon nor Surowiecki specifically discusses the connotation of propaganda, nor the propagandist itself, although both indirectly allude to the concepts. To Le Bon, the crowd's abhorrent nature, along with the likelihood that a powerful leader will arise from the crowd itself, speaks to his value judgement related to propaganda and the propagandist: "The leaders we speak of are more frequently men of action than thinkers. They are not gifted with keen foresight, nor could they be, as this quality generally conduces to doubt and inactivity."[196]

---

[191] James Surowiecki, *The Wisdom of Crowds*, Reprint edition (New York: Anchor, 2005), https://www.amazon.com/dp/B000FCKC3I/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1.

[192] Surowiecki.

[193] Surowiecki.

[194] Surowiecki.

[195] Surowiecki.

[196] Le Bon, *The Crowd*, 116.

Nonetheless, an effective propagandist could likely become Le Bon's "man of action," or the one who breaks up the wise crowd as discussed by Surowiecki. In both cases, the crowd does not necessarily come to the same conclusion it would without the influence of the effective propaganda.

The internet may elicit a new kind of ethos, one of a more technical nature. In 1999, Shane Borrowman (who was, at the time, a teaching associate with the English department at the University of Arizona at Tucson and is now an associate professor of English at the University of Montana Western) looked at the internet's influence on hate speech, specifically Holocaust denial. Borrowman asserted that the internet, unlike profit-driven mediums such as television, radio, or print (looking to identify with the largest possible audience) allows individuals engaged in hate speech to post freely, and also affords them the freedom to "construct their ethos—their credibility or authority."[197] Borrowman breaks the ethos into two categories: an "academic ethos," recognition as an expert in one's field, and the emerging "technical ethos," which is the credibility that comes from the ability to develop professional-looking webpages.[198] While, many websites, in fact, turned the internet into a profit-driven medium (discussed in Chapter III), technical ethos is still worthy of further exploration.

In 2016, Loo Seng Neo and other researchers with the Home Team Behavioural Science Centre in Singapore asserted that it is important to understand how online platforms are used to effectively present extremist material and draw more visitors who spend more time on extremist websites.[199] Neo et al. argue that the most popular online violent extremism platforms mimic the most popular mainstream platforms and offer substantive research to support their assertions.[200] They conclude that the easier it is for users to navigate a website and find the information they are looking for, the more time

---

[197] Shane Borrowman, "Critical Surfing: Holocaust Denial and Credibility on the Web," *College Teaching* 47, no. 2 (Spring 1999): 45.

[198] Borrowman.

[199] Loo Seng Neo et al., "Understanding the Psychology of Persuasive Violent Extremist Online Platforms," in *Combating Violent Extremism and Radicalization in the Digital Era* (Hershey, PA: IGI Global, 2016), 2.

[200] Neo et al., 7.

they will spend on that platform.[201] This concept of technical ethos is often exploited by propagandists to enhance the credibility of their own propaganda. For example, in Macedonia, the fake news factories strive to "make their websites look professional, mimicking legitimate sites with rolling tickers and 'Breaking News' banners."[202]

Pathos, persuading an audience by eliciting emotions or passions, and logos, persuading an audience by reason, also play a role in a message's persuasiveness. In terms of eliciting an emotional response, there is no denying that our current environment speaks more to emotion than to logic. Jenkins, Green, and Ford refer to this phenomenon as spreadable media.[203] The authors describe spreadability as "the potential—both technical and cultural—for audiences to share content for their own purposes, sometimes with the permission of rights holders, sometimes against their wishes."[204] Mihailidis and Viotty build on this concept and explain how we are currently experiencing a "spreadable spectacle."[205] In fact, many argue that we are entering a new paradigm of post-truth.[206]

Luckily for propagandists, even if reason is still at play in persuasiveness, they can leverage existing cognitive factors within the human mind to override the need for reason and increase the persuasiveness of their counterfeit narrative. For example, "confirmation bias" is a phenomenon wherein an individual, usually without being aware of it, more heavily weigh information or evidence that supports his or her prior-held beliefs and

---

[201] Neo et al., 7.

[202] CNN, "The Fake News Machine."

[203] Henry Jenkins, Sam Ford, and Joshua Green, *Spreadable Media: Creating Value and Meaning in a Networked Culture (Postmillennial Pop)*, Kindle edition (New York: NYU Press, 2013), 3, https://www.amazon.com/Spreadable-Media-Creating-Networked-Postmillennial-ebook/dp/B00B1Q88EW/ref=tmm_kin_swatch_0?_encoding=UTF8&qid=1517784651&sr=8-1.

[204] Jenkins, Ford, and Green, 3.

[205] Mihailidis and Viotty, "Spreadable Spectacle in Digital Culture," 443.

[206] Kurt Andersen, "How the U.S. Lost Its Mind," *The Atlantic*, August 7, 2017, https://www.theatlantic.com/magazine/archive/2017/09/how-america-lost-its-mind/534231/; William Davies, "The Age of Post-truth Politics," *New York Times*, August 24, 2016, https://www.nytimes.com/2016/08/24/opinion/campaign-stops/the-age-of-post-truth-politics.html; Amy B. Wang and Amy B. Wang, "'Post-truth' Named 2016 Word of the Year by Oxford Dictionaries," *Washington Post*, November 16, 2016, https://www.washingtonpost.com/news/the-fix/wp/2016/11/16/post-truth-named-2016-word-of-the-year-by-oxford-dictionaries/; "Yes, I'd Lie to You," *The Economist*, September 10, 2016, www.economist.com/news/briefing/21706498-dishonesty-politics-nothing-new-manner-which-some-politicians-now-lie-and.

discounts evidence that is inconsistent with prior beliefs.[207] Similarly, in a phenomenon known as "belief perseverance," when individuals are motivated to defend their current beliefs, they tend to subconsciously take more stock in evidence that supports those beliefs.[208] Studies have shown that once a person takes a stance on a particular issue, he or she tends to maintain and defend that position, whether consciously or subconsciously.[209] Further, people may also actively seek out information that supports their beliefs and avoid information that would refute them.[210] This means that once a person has made up his or her mind, it can be very difficult to change it, even if new evidence proves the existing belief is based on false information.[211]

For example, when Park et al. analyzed messaging on a virtual stock market community, they concluded that the message board users exhibited confirmation bias.[212] Investors treated messages that aligned with their pre-existing beliefs more favorably and, as a result, traded more actively on that information, expecting higher returns than what was necessarily warranted.[213] This calls into question the usefulness of such forums; they may actually lead to overconfidence and decision making based on bias rather than reason.

Confirmation bias is also closely related to a concept called the "backfire effect," which can occur when another person contradicts someone's beliefs. Rather than considering the argument, the individual may "implicitly counterargue against any information that challenges their world view."[214] The individual feels as if he or she is

---

[207] Raymond S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology* 2, no. 2 (1998): 175–220, http://psy2.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf.

[208] Nickerson, 176.

[209] Nickerson, 177.

[210] Nickerson, 177.

[211] Chessen, "Computational Propaganda," 21.

[212] Jaehong Park et al., "Information Valuation and Confirmation Bias in Virtual Communities: Evidence from Stock Message Boards," *Information Systems Research* 24, no. 4 (December 2013): 1050–1067.

[213] Park et al.

[214] Stephan Lewandowsky et al., "Misinformation and its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (December 2012): 119, https://doi.org/10.1177/1529100612451018.

being attacked, and must dispel that feeling by fighting back rather than truly considering the information.[215] Thus, an attempt to debunk misinformation can actually result in reinforcing the very belief you are looking to change.[216] Additionally, if false information or myths are made too familiar—if too many arguments are provided to disprove false information or myths, or if the provided evidence threatens an individual's worldview—the potential backfire effect is even greater.[217]

Confirmation bias and the backfire effect can lead to continued reliance on incorrect information even after the correct information, or a credible retraction, has been provided.[218] Even in error correction, the person may be further reinforcing the misinformation as truth. Swire et al. explain that continually repeating the misinformation in order to correct it could make the false information more familiar, and thus more likely to be considered truth.[219]

Other cognitive factors can also come into play. "Implicit egotism" occurs when recipients are more likely to believe messages because they are being delivered by someone they perceive as being similar to themselves.[220] A "false consensus effect" is a cognitive bias through which people attribute others' views to their own, overestimating the extent to which their views are held in the larger population.[221] The "availability heuristic" is the concept that individuals judge the likelihood, frequency, and extremity of incidents or

---

[215] Lewandowsky et al., 119.

[216] John Cook and Stephan Lewandowsky, *The Debunking Handbook* (St. Lucia, Australia: University of Queensland, 2013), http://sks.to/debunk.

[217] Cook and Lewandowsky, 1.

[218] Briony Swire, Ullrich K. H. Ecker, and Stephan Lewandowsky, "The Role of Familiarity in Correcting Inaccurate Information," *Journal of Experimental Psychology: Learning, Memory, and Cognition* 43, no. 12 (December 2017): 1948–1961, https://doi.org/10.1037/xlm0000422.

[219] Swire, Ecker, and Lewandowsky, 2.

[220] Chessen, "Computational Propaganda," 21.

[221] Chessen, 21; Magdalena Wojcieszak and Vincent Price, "What Underlies the False Consensus Effect? How Personal Opinion and Disagreement Affect Perception of Public Opinion," *International Journal of Public Opinion Research* 21, no. 1 (March 2009): 25–46, https://doi.org/10.1093/ijpor/edp001.

events based on the ease with which those examples come to mind.[222] As is clarified in subsequent chapters, propaganda in the form of counterfeit narratives, laundered through the internet ecosystem, can take advantage of these cognitive biases in a variety of ways, sowing confusion, chaos, and mistrust.

The technique of spreading false misinformation, which goes back centuries and has been leveraged by governments, corporations, and malicious actors alike, can be a powerful force for shaping perceptions, manipulating cognitions, and directing behavior. And while it is true that the message must be persuasive in order to effect positive change, persuasion and propaganda are not the same. In persuasion, the goal is to obtain achievement of mutual needs; propaganda, however, benefits only the propagandist, often at the expensive of the individuals exposed to it. Counterfeit narratives, therefore, help frame propaganda in a way that more accurately describes this phenomenon's pervasiveness. Counterfeit narratives, however, are not effective on their own; they must be passed through the internet ecosystem, and the most effective among them take advantage of technology to spread even wider and more rapidly. Today, propagandists can rely on existing processes developed to improve the customization, ease of access, and availability of information online to passively or actively help their counterfeit narratives go viral.

[222] Amos Tversky and Daniel Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology* 5 (1973): 207–232, https://msu.edu/~ema/803/Ch11-JDM/2/TverskyKahneman73.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ECHO CHAMBERS AND ADVERTISING AND BOTS ... OH MY!

A counterfeit narrative that no one sees does very little to push the propagandist's agenda. It is therefore important to identify strategies used to spread the narrative rapidly and effectively. As discussed in this chapter, the internet ecosystem itself can enable the spread and inaccurate validation of counterfeit narratives. Further, that ecosystem fosters a number of processes that can accelerate the spread of propaganda. These processes are the focus of this chapter.

Before discussing the aspects of today's internet that are potentially worrisome from a propaganda standpoint, it is important to understand how we created our current online society. Today's online ecosystem looks very different than it did even ten years ago, and it is almost unrecognizable from the original 1980s ecosystem. Design for the Transmission Control Protocol/Internet Protocol (TCP/IP) on which today's internet is based began in 1973 and became operational in 1983.[223] In the beginning, the internet was used primarily by the military and academia, and only individuals connected to related institutions readily accessed it.[224] Beginning in the early 1990s, when it first became privatized, the internet slowly began to trickle into mainstream society. It eventually became the ubiquitous and unavoidable force that it is today—one that American society perhaps takes for granted (except when it stops working).[225] Naughton likens the internet to a utility upon which our society is utterly dependent, but which most people poorly understand.[226] He argues that the internet is now a "general purpose technology," which, as defined by Bresnehan, means "(i) it is widely used; (ii) it is capable of ongoing technical improvement; and (iii) it enables innovation in application sectors."[227]

---

[223] John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," *Journal of Cyber Policy* 1, no. 1 (January 2016): 5, https://doi.org/10.1080/23738871.2016.1157619.

[224] Naughton, 5.

[225] Naughton, 5, 11.

[226] Naughton, 5.

[227] Naughton, 16–17.

Two key features allowed the internet to hit mainstream audiences. First is the internet's commercialism, which was created when its architecture was privatized to internet service providers (ISPs).[228] This allowed laypersons an easy way to access the internet—first via a slow dial-up connection and later through fiber-optic cables. The second feature was the development of the "World Wide Web," which allowed users to publish, find, and retrieve "documents" (i.e., webpages) stored around the world on various servers.[229] This was followed by web browsers, which can display graphics within a webpage, removing the need for the user to open a separate window to view pages.[230] This seemingly small change helped developers realize the internet's potential entertainment value.[231] Thus followed the infamous "dot-com bubble" as companies quickly took advantage of rising consumer interest in the internet. While the boom was short-lived for many dot-com companies, this bubble led to technological infrastructure, such as large fiber-optic cable networks and server farms that were ultimately needed "to hasten the maturation of the network."[232]

Around 1993, the internet transitioned from a primarily one-way producer–consumer cyberspace to a highly integrated and immersive social exchange platform.[233] Before this time, the internet did not afford users the ability to interact with or personalize webpages, to find readers who visited the same page, or simply to collaborate with others via the Web.[234] This impasse was overcome by cookies, secure http protocol (HTTPS), specialized plugins, and JavaScript; although these tools at times seemed ad hoc, they

---

[228] Naughton, 13, 15.

[229] Naughton, 13; Jose van Dijck, *The Culture of Connectivity: A Critical History of Social Media*, 1st edition (Oxford: Oxford University Press, 2013), 9, https://www.amazon.com/Culture-Connectivity-Critical-History-Social-ebook/dp/B00AWOTA96/ref=mt_kindle?_encoding=UTF8&me=.

[230] Naughton, "The Evolution of the Internet," 14.

[231] Naughton, 14.

[232] Naughton, 15.

[233] Doug Divine, Toni Ferro, and Mark Zachry, "Work through the Web: A Typology of Web 2.0 Services," in *Proceedings of the 29th ACM International Conference on Design of Communication* (2011): 121–28; Naughton, "The Evolution of the Internet," 16–17.

[234] Naughton, "The Evolution of the Internet," 16.

became the foundation of what was eventually dubbed "Web 2.0."[235] Tools such as Google's PageRank algorithm (computer code that uses an automated peer review to rank webpages) and websites such as Wikipedia (a crowd-sourced encyclopedia) "harnessed the collective intelligence available on the Web."[236] At the same time, features like Amazon's product peer review exploited users' willingness "to engage with the enterprise."[237]

Another key feature of Web 2.0 was that users could create content freely and with no financial incentive.[238] Further, many new online services were interconnected through application programming interfaces, which connect major web services, such as Google Maps, with other data sources and services created by other parties.[239] Many services on Web 2.0 were never considered finished, but rather seen as continuous "works in progress" that could be updated, upgraded, and edited as needed. Finally, because the World Wide Web offered a common programming standard, and because its services and webpages could typically bypass firewalls, companies began to see the Web as a viable platform for their services.[240]

Around 2001, the features of Web 2.0 combined with the rising use and connectivity of smartphones, significantly altering the way people used and accessed the internet.[241] As Web 2.0 continued to mature, users began to program platforms and services for specific objectives.[242] Jose van Dijck, professor of comparative media studies and former dean of the University of Amsterdam, argues that, at this point, online services were no longer simply a utility; they had become a customized service—like water that was once available only through pipelines, but is now distributed as bottles of Evian or through a water-filtering system. Unlike websites before this transition, which "generally

---

[235] Naughton, 16.

[236] Naughton, 16.

[237] Naughton, 16.

[238] Naughton, 17.

[239] Naughton, 17.

[240] Naughton, 17.

[241] Naughton, 17.

[242] van Dijck, *Culture of Connectivity*, 4.

operated as *conduits* for social activity, the new platforms increasingly turned these conduits into *applied services*, rendering the Internet easier to use but more difficult to tinker with."[243] This means that social media platforms are not merely facilitators of networking activities: we must understand how the these platforms interact with social practices online.

After the Web 2.0 boom, emerging social media platforms and technology companies soon offered services such as web search and social networking free of charge.[244] In exchange, whether users were aware or not, the service providers were then authorized, through terms of service agreements, to "gather data about [the customers] based on their online behaviour and use the resulting knowledge to target advertising at them."[245] This business plan was a lucrative one; digital corporations such as Google and Facebook have come to dominate the internet over the past twenty years, wielding significant influence and power over billions of people's lives.[246]

In fact, in 2014, Facebook, Inc., and Cornell University published a study about "massive-scale emotional contagion through social networks" and demonstrated the impact Facebook could have on users' emotions.[247] In the study, Facebook varied the extent to which over 650,000 users were exposed to expressions of emotion in their News Feeds. Researchers then recorded if the exposure to such content impacted the content that the affected users posted. In other words, if a user was exposed to a higher amount of negative emotional content, would he or she tend to post more negative content themselves? And then would *others* who saw those posts also post negative emotional content? This is

---

[243] van Dijck, 4.

[244] Naughton, "The Evolution of the Internet," 18; Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, Reprint edition (New York: Anchor, 2016), 69, https://www.amazon.com/Future-Crimes-Digital-Underground-Connected/dp/0804171459/ref=sr_1_1?ie=UTF8&qid=1517711962&sr=8-1&keywords=future+crimes; van Dijck, *Culture of Connectivity*, 4.

[245] Naughton, "The Evolution of the Internet," 18; Goodman, *Future Crime*, 69; van Dijck, *Culture of Connectivity*, 4.

[246] Naughton, "The Evolution of the Internet," 19.

[247] Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences of the United States of America* 111, no. 24 (June 2014): 8788–8790, https://doi.org/10.1073/pnas.1320040111.

described as emotional contagion.[248] The study results suggested that emotions expressed in content posted by friends and loved ones online do, in fact, influence the moods of the users who interact with that content. This is an important realization when considering that social movements, outrage, and large gatherings are often initiated online. If a person or organization has access to these algorithms, or has the money to pay those who have access to them, that person or organization could generate a desired emotional state among the platform's users. While this finding is already concerning on its own, the journal that published the study expressed an even more alarming concern.[249] The journal's editor in chief wrote: "It is nevertheless a matter of concern that the collection of the data by Facebook may have involved practices that were not fully consistent with the principles of obtaining informed consent and allowing participants to opt out."[250]

Facebook, Inc., indicated that all individuals who accept their terms of service give up the right to opt out of such research.[251] The study's findings, and Facebook's attitude when it comes to user consent, raise concern about other ways that Facebook and other technology companies do, or could, impact user behavior. In 2015, Robert Gehl, a professor at the University of Utah, described the potential risk to free speech and democracy posed by these big online conglomerates, which he dubs "corporate social media."[252] Gehl asserts that these platforms, while offering users the ability to produce content, are also "for-profit firms who can be hostile to alternative ideas, discourses, and organizing—especially when those practices challenge corporate hegemony."[253]

Other researchers and public figures have raised similar concerns. Tristan Harris, a former Google product manager turned design ethicist, argues that for-profit technology companies have hijacked our minds in an effort to convince us to spend more and more

---

[248] Kramer, Guillory, and Hancock, 8788.

[249] Kramer, Guillory, and Hancock.

[250] Kramer, Guillory, and Hancock.

[251] Kramer, Guillory, and Hancock.

[252] Robert W. Gehl, "The Case for Alternative Social Media," *Social Media+ Society* 1, no. 2 (July–December, 2015): 1.

[253] Gehl, 1.

time on their platforms.[254] Harris posits that these companies are now controlling the minds of billions of people; although their purpose is not necessarily nefarious, they are taking advantage of these resources to garner attention and thus make even more profit.[255] While researchers, government stakeholders, and society at large are just beginning to understand the opportunities and threats these technologies pose, when it comes to propaganda promulgation, law enforcement, policymakers, and the general public need to be aware of important current and emerging processes.

This chapter discusses prevalent tools that could be accelerating the spread of counterfeit narratives online. It concludes by examining emerging technologies that may impact both the counterfeit narratives themselves and the internet ecosystem in the future. It is important to note that these tools are not used solely to spread counterfeit narratives. Most were created for other purposes, and have been hijacked or leveraged by bad actors.

A. ECHO CHAMBERS

Over the past several years, social media and other technology platforms have begun to leverage algorithms to personalize content according to the interests and tastes of their users.[256] Google, for example, uses personalized search results; now, "instead of having to sift through pages of results you have no interest in, Google will custom fit the results displayed based on your past search history and general Web surfing habits."[257] While the search results are often relevant, they "might restrict the breadth of sites that are delivered to the user leading searchers to only see sources of information that they typically agree with, which deals with cognitive dissonance in a detrimental way for society at

[254] Nicholas Thompson et al., "Our Minds Have Been Hijacked by Our Phones. Tristan Harris Wants to Rescue Them," *Wired*, July 26, 2017, https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/.

[255] Tristan Harris, "How a Handful of Tech Companies Control Billions of Minds Every Day," TED video, April 2017, https://www.ted.com/talks/tristan_harris_the_manipulative_tricks_tech_companies_use_to_capture_your_attention.

[256] Alessandro Bessi et al., "Users Polarization on Facebook and YouTube," *PloS One* 11, no. 8 (August 2016): 1.

[257] "Google Personalized Results Could Be Bad for Search," PCWorld, December 7, 2009, http://www.pcworld.com/article/183891/Google_Personalized_Results_Could_Be_Bad_for_Search.html.

large."[258] Facebook is doing the same thing on its users' News Feeds, often prioritizing posts from a user's closest friends and family (who in many cases have similar viewpoints as the user) or sites the user has visited or liked. Without realizing it, an individual may "develop tunnel vision when the personalization is based on … past click and like behavior."[259] Bessie et al. and Vicario et al. refer to this phenomenon as the creation of "echo chambers," while Gossart refers to it as "information cocoons."[260]

An echo chamber is created when a user only consumes online content that agrees with his or her existing viewpoint, thus reinforcing that viewpoint.[261] Some researchers warn that a platform's algorithm, or a search engine tailored to filter results based on the user's interests, tastes, or opinions, could result in echo chambers, thus creating an environment in which the user cannot *choose* to ignore dissenting views; the user is simply never exposed to dissenting views at all.[262] Other studies suggest that confirmation bias, discussed in Chapter II, is a major factor driving users' adherence to echo chambers and the resulting polarization.[263] In 2016, Bessi et al. conducted a research study about user polarization on Facebook and YouTube by examining videos posted to sites on science-based and conspiracy theory webpages (conflicting narratives).[264] Researchers analyzed the behavior of over twelve million users, comparing consumption patterns for both types of videos in an attempt to determine if, and how, users become polarized from comment to comment. They determined that content was the polarizing factor. Echo chambers were

---

[258] PCWorld.

[259] Nelson Granados, "How Facebook Biases Your News Feed," *Forbes*, June 30, 2016, http://www.forbes.com/sites/nelsongranados/2016/06/30/how-facebook-biases-your-news-feed/.

[260] Cedric Gossart, "Can Digital Technologies Threaten Democracy by Creating-Information Cocoons," in *Transforming Politics and Policy in the Digital Age*, ed. Jonathan Bishop (Hershey, PA: IGI Global, 2014), 145–154.

[261] Seth Flaxman, Sharad Goel, and Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly* 80, Special Issue (2016): 299.

[262] Gossart, "Digital Technologies Threaten Democracy."

[263] Bessi et al., "Polarization on Facebook and Youtube," 2.

[264] Bessi et al., 2.

established independent of the platform or the algorithm that promoted content. Instead, it was conflicting narratives that led users to form "homogeneous echo chambers."[265]

Regardless of how echo chambers form, what results are social subgroups online that only share information with like-minded people.[266] As a result, "these technologies might impoverish democratic debate and reduce exchanges amongst the stakeholders of a given political arena while radicalising their points of views."[267] These often financially motivated mechanisms created by technology corporations to deliver customizable content have actually made it easier for propagandists to contain and control information, whether intentionally or unintentionally, to enhance propaganda. A propagandist could manipulate the echo chamber to spread messaging and content that benefits his or her agenda. These tactics are reinforced by cognitive factors such as confirmation bias, implicit egotism, and the false consensus effect (described in Chapter II).

B. ONLINE ADVERTISING

With the growing number of social media and other internet platforms that use advertising to gain profit in the online world, these platforms have become increasingly automated—they are engineered to track and identify their users' interests.[268] This means that social media platforms are not just enabling or facilitating social activity, they are helping to *shape* them.[269] As a result, online advertising may play a significant role in the spread and proliferation of counterfeit narratives.

Online advertising today is often targeted to specific individuals. In the past, a company would have to determine which sites it wanted to use for advertising. Today, companies typically rely on an "automated advertising—a system that matches ads to anonymized profiles of consumers, based on data like what they have searched for."[270] To

---

[265] Bessi et al., 7.

[266] Gossart, "Digital Technologies Threaten Democracy."

[267] Gossart.

[268] van Dijck, *Culture of Connectivity*, 11.

[269] Jowett and O'Donnell, *Propaganda & Persuasion*, 15.

[270] Subramanian, "Inside the Macedonia Fake-News Complex," 10.

put this in perspective, consider grocery checkout lines, which are stocked with candy, soda, and other treats marketed to entice average consumers, or their children. Personalized online advertising stocks those same checkout shelves with items that you personally (or your child) have been interested in or have bought in the past. This increases the likelihood that you will purchase an item. These companies are making historic profits, especially in the United States, and are far from transparent when explaining how their algorithms and online advertising mechanisms work.[271] It is no longer services that are the commodity; it is the consumer.

For example, in 2016 and 2017, Facebook's automated advertising platform earned the company more than 44 billion dollars in revenue.[272] Facebook has been building and modifying its advertising mechanism for over a decade, beginning with a product called Beacon that tracked users' website activity and then partnered with the sites to have the information sent back to Facebook.[273] Facebook would then post something to the user's profile based on the content of recently visited sites (on the user's behalf but without his or her consent).[274] For example, if a user recently purchased a product on Amazon, Facebook would post this activity on the user's timeline.[275] Immediate backlash ensued; although Facebook promised users they could opt out, Facebook was still keeping the information collected from these sites.[276]

During the 2016 U.S. presidential election, Russian actors leveraged a number of social media platforms, including Facebook, where they spent over $100,000 in advertising.[277] These advertisements are believed to have reached over 126 million

---

[271] van Dijck, *Culture of Connectivity*, 11.

[272] "Facebook's Reckoning & Free Money in Finland: VICE News Tonight Full Episode (HBO)," YouTube video, uploaded by VICE News, November 7, 2017, 4:55–14:15, https://www.youtube.com/watch?v=ACiXq_lBWlY&list=PLw613M86o5o5h_7QkuryiioEJDG0eI07V&index=20.

[273] VICE News, 4:55–14:15.

[274] VICE News, 4:55–14:15.

[275] VICE News, 4:55–14:15.

[276] VICE News, 4:55–14:15.

[277] Digital Shadows, "The Business of Disinformation," 10; VICE News, "Facebook's Reckoning."

Facebook users.[278] At first, Facebook and other social media platforms denied that their advertising algorithms played a role in the outcome of the presidential election; however, they quickly changed their tune, admitting that foreign election interference may have existed on the platform.[279] Beginning around 2015, Russian co-conspirators were spending thousands of dollars per month to promote social media groups and messages created by the Internet Research Agency, LLC.[280] In the 2018 indictment of thirteen Russians affiliated with the Internet Research Agency, prosecutors specifically pointed to a number of political advertisements on social media platforms that were purchased by these subjects using false names of U.S. persons and entities.[281]

Another example involves Facebook's use of a service called Instant Articles, which provides publishers a way for "their articles to load quickly and natively within the Facebook mobile app."[282] In return, publishers can insert advertisements, either their own or using Facebook's ad network, which earns Facebook a share of the revenue.[283] While many trustworthy and credible publishers have decided to opt out of Instant Articles, spammers and fake news generators, especially those overseas, continue to leverage the service.[284] This means that Facebook itself may be benefiting financially from the spread of counterfeit narratives.[285] Tristan Harris, during an April 2017 TED talk, described this phenomenon of targeted advertising for profit and its influence on human behavior. Harris stated, "You can precisely target a lie directly to the people who are most susceptible. And

---

[278] Digital Shadows, "The Business of Disinformation," 10; VICE News, "Facebook's Reckoning."

[279] VICE News, "Facebook's Reckoning," 4:55–14:15.

[280] United States of America v. Internet Research Agency LLC 18 U.S.C. § § 2, 371, 1349, 1028A (D.C. Dist. Columbia 2018), 14, https://www.justice.gov/file/1035477/download.

[281] United States of America v. Internet Research Agency, 4.

[282] Jane Lytvynenko, "Big Publishers Are Abandoning Instant Articles but Fake News Spammers Are All in," BuzzFeed, accessed February 7, 2018, https://www.buzzfeed.com/janelytvynenko/fake-news-in-instant-articles.

[283] Lytvynenko.

[284] Lytvynenko; Pete Brown, "More than Half of Facebook Instant Articles Partners May Have Abandoned it," *Columbia Journalism Review*, February 2, 2018, https://www.cjr.org/tow_center/are-facebook-instant-articles-worth-it.php.

[285] Lytvynenko, "Big Publishers."

because this is profitable, it is only going to get worse"[286] This, Harris argues, is the greatest threat to humanity. Any issue, problem, or threat we need to tackle requires us to focus our attention on that topic; but if we are continuously distracted by these algorithms online, which are maximized to achieve one thing (profits for the technology companies), we will be unable to act on any important matter.[287]

Despite the overwhelming controversy surrounding the social media vendors and other online platforms, these companies continue to harvest, collate, and sell user data pretty much the same way they always have.[288] Advertising is big business: an U.S.- or Canada-based Facebook user is worth three times the amount of a user in any other country, which creates a resounding financial incentive to maintain the status quo.[289]

But the concern over advertisements and user tracking runs deeper. Mark Goodman, a former FBI cybercrimes agent and author, stated, "Purveyors of 'free' Internet services persistently track users across their entire online experience as well as their movements in the physical world through the use of their mobile phones."[290] Americans and other Westerners typically carry their mobile phones with them everywhere, which has massive implications on the impact of corporate surveillance and its ability to manipulate our behavior. Researchers, privacy advocates, and legislators should be very concerned about major technology corporation's efforts to track user activity both online and off, and with what appears to be very little regulation.

---

[286] Harris, "Handful of Tech Companies," 5:58.

[287] Harris, 13:04.

[288] "Amid Facebook's Troubles, Message to Advertisers Stays Consistent," *New York Times*, September 28, 2017, https://mobile-nytimes-com.cdn.ampproject.org/c/s/mobile.nytimes.com/2017/09/28/business/media/facebook-advertising-week.amp.html.

[289] Silverman and Alexander, "Teens in the Balkans"; Anita Balakrishnan, "Facebook Made about $4.23 off Your Profile in the First Three Months of the Year," CNBC, May 3, 2017, www.cnbc.com/2017/05/03/facebook-average-revenue-per-user-arpu-q1-2017.html.

[290] Goodman, *Future Crimes*, 452.

C. BOTS AND COMPUTATIONAL PROPAGANDA

Another form of automation, platform- and user-controlled bots, also plays a major role in internet services' effectiveness and capabilities. A bot is piece of computer code programmed to do a particular task. A botnet is "a group of bots that are created and centrally controlled by a master, called 'botmaster.'"[291] Automated bots can monitor whether or not a website is functioning properly, collect information for a search engine, or fetch website content for mobile and web applications.[292] However, researchers are just beginning to study the nefarious use of automation, especially in regards to bots deployed by social media users.

Imperva Incapsula, a web cloud services provider, recently estimated that bots make up 51.2 percent of all internet traffic.[293] As many as 48 million Twitter accounts (15 percent of accounts) are believed to be bots.[294] Imperva Incapsula breaks the types of bots into eight categories; it describes four of the eight as "good bots" and four as "bad bots."[295] The "bad bots" are described as impersonators: bots that assume false identities often, with the intent of bypassing security; scrapers; bots that extract data from websites without authorization; spammers; bots that inject links to spam into comment sections and other online forums; and hacker tools, or bots that look for potential vulnerabilities in websites in an effort to exploit them.[296] Impersonator bots are the type used most frequently, and the ones of most concern for the spread of counterfeit narratives online. Impersonator bots are designed to gain access to websites and other platforms as if they were human. These bots can be further broken down into several categories:

---

[291] Juan Echeverría and Shi Zhou, "The 'Star Wars' Botnet with >350k Twitter Bots," Cornell University Library, June 13, 2017, 1, https://arxiv.org/abs/1701.02405.

[292] Igal Zeifman, "Bot Traffic Report 2016," *Incapsula* (blog), January 24, 2017, www.incapsula.com/blog/bot-traffic-report-2016.html.

[293] Freedom House, "Manipulating Social Media," 9.

[294] Samuel C. Woolley, "Computational Propaganda and Political Bots: An Overview," in *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, ed. Shaun Powers and Markos Kounalakis (Washington, DC: United States Advisory Commission on Public Diplomacy, 2017), 13.

[295] Zeifman, "Bot Traffic Report 2016."

[296] Zeifman.

- **Follower bots** use fake accounts, often purchased, to increase the number of "people" following a given account or a given post.[297] Both nefarious and benign actors use this type of bot frequently in order to have more of an impact online. Much of one's quantifiable value on the internet is tied to a concept called the "popularity principle," which explains that "the more contacts you have and make, the more valuable you become, because more people think you are popular and hence want to connect with you."[298] The same can be true for bots that "like" or promote a specific post. That posts garners more interest and seeming endorsement, and may therefore inherit more credibility.

- **Roadblock bots** are used to undermine trending hashtags by associating them with oppositional or irrelevant information. The ultimate effort is to shut down the hashtag, making it more difficult for advocates to reach their followers.[299]

- **Propaganda bots** are bots used to influence and persuade users online by spreading any combination of truths, half-truths, and falsehoods in relatively quick succession.[300] Nation-states have used these bots to "combat anti-regime speech and promote the ideas of the state."[301]

Many researchers now refer to impersonator bots used to spread disinformation as computational propaganda.[302] Systematic research of computational propaganda has only just begun. In July 2017, researchers from Indiana University at Bloomington claimed to

---

[297] Digital Shadows, "The Business of Disinformation," 9; Woolley, "Computational Propaganda," 16.

[298] van Dijck, *Culture of Connectivity*, 12.

[299] Woolley, "Computational Propaganda," 16; Chessen, "Computational Propaganda," 20.

[300] Chessen, "Computational Propaganda," 20.

[301] Woolley, "Computational Propaganda," 16.

[302] "Security experts argue that more than 10 percent of content across social media websites, and 62 percent of all web traffic, is generated by bots—pieces of computer code that automate human tasks online." Woolley, 13.

have conducted the first study to systematically, rather than anecdotally, "study the spread of fakes news by social bots."[303] However, the Oxford Internet Institute, "a multidisciplinary research and teaching department of the University of Oxford, dedicated to the social science of the Internet" may have pre-dated this work. The Oxford Internet Institute, through the Computational Propaganda Research Project, defined and studied computational propaganda, "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks."[304] The Computational Propaganda Research Project

> researched the use of social media for public opinion manipulation. The team involved 12 researchers across nine countries who, altogether, interviewed 65 experts, analyzed tens of millions of posts on seven different social media platforms during score of elections, political crises, and national security incidents. Each case study analyzes qualitative, quantitative, and computational evidence collected between 2015 and 2017 from Brazil, Canada, China, Germany, Poland, Taiwan, Russia, Ukraine, and the United States.[305]

Published research by Kate Starbird, an assistant professor from the University of Washington, also predated the Indiana University study. Starbird's research, which she eventually published, was first presented at the International Conference on Web and Social Media in May 2017. Her goal was to provide a "systematic lens for exploring the production of a certain type of 'fake news'—*alternative narratives* of man-made crisis events."[306] Regardless of who came first, the research on automation continues to be relevant, cutting-edge, and emerging.

---

[303] Shao et al., "The Spread of Fake News by Social Bots."

[304] Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary" (working paper, University of Oxford, 2017), 3, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

[305] Woolley and Howard, 3.

[306] Kate Starbird, "Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter" (paper presented at the 11th International Conference on Web and Social Media, Montreal, Canada, May 15–18, 2017).

Bots associated with computational propaganda can range from simple pre-programmed phrases to more advanced smart bots that incorporate machine learning.[307] Bots, especially politically oriented bots, are present and active in many social media conversations, and are considered by some to be "amongst the most important recent innovations in political strategy and communication technology."[308] The transparency of the technology is also important. Woolley offers three categories of transparency, 1) transparent bots—those that identify themselves or are labeled as bots, 2) semi-transparent bots—those that are human-like but claim to be bots, and 3) non-transparent bots, which attempt to pass as human users.[309] All three types of bots are used by a wide number of actors, including corporations, hackers, politicians, state-sponsored groups, and terrorist organizations.[310]

Phenomena like computational propaganda are additional tools used by propagandists to enhance and challenge the spread and believability of counterfeit narratives. Terrorists, hate groups, and adversarial nation-states use these tools to "spread their messages of intolerance, to suppress opposition efforts, and to identify new recruits."[311] In their 2017 working paper, Woolley and Guilbeault analyzed approximately 17 million tweets and over 1.5 million unique users between November 1 and November 11, 2016. They concluded that political bots deployed during this time did have an influence on the political discussions around the 2016 U.S. presidential election.[312] The 2017 report by Freedom House on internet freedom also identified this concern:

> In at least 20 countries, characteristic patterns of online activity suggested the coordinated use of such "bots" to influence political discourse. Thousands of fake names and profiles can be deployed with the click of a mouse, algorithmically programmed to focus on certain critical voices or

---

[307] Woolley, "Computational Propaganda," 14.

[308] Woolley, 14.

[309] Woolley, 15.

[310] Chessen, "Computational Propaganda," 19.

[311] Chessen, 19.

[312] Woolley and Guilbeault, "Computational Propaganda, 14.

> keywords. They are capable of drowning out dissent and disrupting attempts to mobilize collective action online.[313]

Computational propaganda such as twitter bots can be used to influence an audience's judgement by manipulating the number, volume, and variety of endorsements. Bots can be used to fake trending topics and manipulate public opinion. Twitter bots can "tweet like real users, but coordinated centrally around a specific topic. They [can] also post positive or negative tweets skewing metrics used by companies and researchers to track opinions on that [topic]."[314] The bots may "orchestrate a campaign to create a false sense of agreement" among users, a technique called astroturfing, making it seem like the idea stemmed from the particular online community when it actually began with coordinated bots.[315] Twitter bots have also been used to develop fake followers for other Twitter users. Individuals can buy and sell Twitter followers to make it seem as if they have more influence or power.[316] This has direct application for the concept of authority: people who have more followers on Twitter seemingly have more influence, credibility, and impact.

Propagandists can use bots to undermine the credibility of legitimate sources by making illegitimate content appear as if it has come from a large volume and variety of sources, and that it has been endorsed by many users.[317] Bots can also leverage cognitive factors like implicit egotism—the bots can mimic the target audience and create a false consensus effect if the bots overwhelm the true grassroots conversation.[318] Freedom House mentioned this phenomenon in its 2017 report on internet freedom, discussing the tactics many governments use to manipulate crowdsourcing and mimic grassroots efforts. The report stated, "It can be hard to distinguish propaganda from actual grassroots nationalism,

---

[313] Freedom House, "Manipulating Social Media," 9.

[314] Echeverría and Zhou, "The 'Star Wars' Botnet."

[315] Echeverría and Zhou, 2.

[316] Echeverría and Zhou, 2.

[317] Chessen, "Computational Propaganda," 20.

[318] Chessen, 20.

even for seasoned observers."[319] While bots may appear harmless, even when deployed through computational propaganda, this technology could have massive implications for free speech and for the public's ability to form true consensus.

D. ADDITIONAL EMERGING TECHNOLOGIES

With the emergence of artificial intelligence, many researchers believe we will see more propaganda campaigns and disinformation over the next few years. Matt Chessen, a researcher at the Atlantic Council and policy advisor at the Department of State, refers to this new phenomenon as MADCOMs, which he defines as "the integration of [artificial intelligence] systems into machine-driven communications tools for use in computational propaganda."[320] Chessen argues that MADCOMs will have an even greater influence on internet users' beliefs because they can develop extremely targeted and highly personalized propaganda from the data points already available through social media, internet web-browsing, frequent shopper cards, and many other sources.[321] As we have seen with online advertising, these MADCOMs will become increasingly capable of inferring "your personality, political preferences, religious affiliation, demographic data, and interests."[322] Rather than using bots, which have to be programmed by a human, MADCOMs' artificial intelligence could dynamically generate content and information in real-time, specific to each user.[323]

Additionally, the emerging ability to edit both video and audio directly within a clip has some astounding implications for future counterfeit narratives. One product, Adobe Voco, has even been described as the "Photoshop of speech."[324] Voco can take a twenty-

---

[319] Freedom House, "Manipulating Social Media," 9.

[320] Matt Chessen, *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, And Threaten Democracy ... And What Can Be Done about it* (Washington, DC: Atlantic Council, 2017), http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.

[321] Chessen, 2.

[322] Chessen, 3.

[323] Chessen, 3.

[324] "'Photoshop for Voice' Faces Backlash," BBC, November 7, 2016, http://www.bbc.com/news/technology-37899902.

minute audio sample of a person's voice and insert new words or phrases that mimic the person's speech patterns.[325] Google has a similar product called Wavenet. Similar technologies are being developed to replicate faces in order to produce fake videos. Products such as Pinscreen, which creates user-generated personal avatars, and Face2Face offer glimpses into the technology to come.[326] These tools are currently in their infancy; right now, it is easy to recognize the difference between an avatar and an actual human face. However, the technology will continue to advance and become more sophisticated.

Already today, these technologies are being leveraged online to create videos that depict people doing things they never actually did. For example, in line with the popular internet adage "if it exists, there is porn of it," users have started creating fake pornography videos, coined "deepfakes," that swap the faces of pornography stars with those of celebrities.[327] Anyone with an understanding of predictive algorithms and deep learning can leverage open-source tools and algorithms to make deepfakes.[328] In fact, the practice has become so common that some online producers have started to worry their content may be used to create fake child porn, because the datasets of images they are using contain images of the celebrities as minors.[329]

These sorts of technologies could soon have enormous implications for the development and rapid spread of powerful counterfeit narratives. Bloggers have already been discussing these implications: one group of bloggers demonstrated what they call the "future of fake news," posting a sample video to the website futureoffakenews.com.[330] When the website loads, you see a video of former President Barack Obama giving a

---

[325] BBC.

[326] Pinscreen, accessed February 3, 2018, https://www.pinscreen.com/; "Face2Face: Real-Time Face Capture and Reenactment of RGB Videos," Visual Computing Group, June 2016, www.niessnerlab.org/projects/thies2016face.html.

[327] Samantha Cole, "AI-Assisted Fake Porn Is Here and We're All Fucked," *Motherboard*, December 11, 2017, https://motherboard.vice.com/en_us/article/gydydm/gal-gadot-fake-ai-porn.

[328] Cole.

[329] Samantha Cole, "Fake Porn Makers Are Worried about Accidentally Making Child Porn," *Motherboard*, February 27, 2018, https://motherboard.vice.com/en_us/article/evmkxa/ai-fake-porn-deepfakes-child-pornography-emma-watson-elle-fanning.

[330] Future of Fake News, accessed September 10, 2017, http://futureoffakenews.com/.

weekly presidential address, in which he states, "The single most important thing I could do is play golf."[331] While it is visually clear that the video has been modified, the audio is indiscernible from something President Obama actually said.

This technology's ability to bolster counterfeit narratives seems almost endless. Imagine writing a false article on a false website claiming that future President "John Smith" just stated, "All white people deserve to die." Then you can back up this false claim with a modified video of the *real* President John Smith in which he appears to be uttering the false statement. Another example: An edited version of a law enforcement encounter begins to circulate online. The original video of the true-to-life account shows a subject pointing a weapon at an officer, who then fatally shoots the subject. However, the video is altered to make it appear as though the subject is cooperating with law enforcement and is unarmed. This creates a strong counterfeit narrative that the officer acted unlawfully.

Propagandists will be able to create fake videos of natural disasters, explosions, riots, or mass shootings that look so close to the real thing that it will take time and forensic analysis to decipher the differences. Considering the speed at which counterfeit narratives move online, coupled with cognitive biases such as the backfire effect, defeating these sorts of lies may prove incredibly difficult. Echo chambers are developed within social constructs; computational propaganda and online advertising are only effective because they cater to processes that already exist within the human brain and in humans' interactions with each other. Add emerging technologies such as artificial intelligence and video/audio editing, and the future of fake news is worrisome.

All of these online processes, algorithms, and technologies can be leveraged to undermine the legitimacy of cognitive strategies that reasonable people use, both consciously and subconsciously, to ascertain the facts of an argument. If we implant this technology into an online ecosystem that is susceptible to counterfeit narratives, a process emerges—one that is both astounding and troubling. This process is called information laundering.

---

[331] Future of Fake News.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INFORMATION LAUNDERING: OR HOW TO CHEAT THE SYSTEMS

The current internet ecosystem—in which consumers can not only easily find information, but also contribute to it—creates a very influential environment. It allows truthful, important information to spread at previously impossible rates, but at the same time opens up the floodgates for the rapid spread of counterfeit narratives. Propagandists can use online technologies such as computational propaganda, echo chambers, and advertising to further cheat the internet ecosystem and create and spread content that is more influential and believable. Committed actors can leverage these techniques to intentionally undermine the credibility of legitimate sources by leveling the playing field for subversive, often extremist, content that masquerades as credible content in the public debate.

A. INFORMATION LAUNDERING: AN INTRODUCTION

In 2012, Adam Klein, then a humanities, communication studies, and public relations professor at Mercy College in New York and now an assistant professor at Pace University, studied how the internet offers extremist groups (particularly white nationalist and supremacist groups) "the perception of legitimacy."[332] During his research, Klein noted: "These communities intend to impact the way that white society *thinks* about the 'nonwhite' society. Their goal is to digitally introduce a legitimate campaign of 'racial enlightenment' into the mainstream discourse of the web—to corrupt it.[333]

Klein observed that a large number of "hate websites" had grown substantially since 2007 and increased traffic flow to these websites created "a revitalized and highly vocal hate movement" in the United States.[334] These hate groups used the unique aspects of the internet ecosystem to intertwine their rhetoric with similar, mainstream ideology until they converged, making them hard to distinguish. While this observation is troubling,

[332] Klein, "Slipping Racism into the Mainstream," 429.

[333] Klein, 432.

[334] Klein, 428.

Klein's more important observation was related to *how* these groups were effectively spreading their rhetoric. Klein argued that we must look beyond the impact of any single platform or technology and instead focus on the entirety of the internet and how it can be used to normalize fringe or extremist ideology.[335] He argues that hate speech should not be considered a rhetorical strategy, but rather a "tactical employment of words, images, and symbols, as well as links, downloads, news threads, conspiracy theories, politics, and even pop culture, all of which have become the complex machinery of effective inflammatory rhetoric."[336]

Political science scholars have also noted this phenomenon. In his book *Right-Wing Critics of American Conservatism*, University of Alabama Assistant Professor George Hawley notes: "Racism online is not isolated to expressly racist websites. Such sentiments often find their way into mainstream news and commentary via open comments sections. Much of this is spontaneous, but there is also a larger campaign to hijack these discussions and push them in a more racial direction."[337]

Klein argues that this rhetoric denigrates a selected group, in this case non-white individuals, in an effort to appeal to the mentality of the majority, in this case white individuals, and, in doing so, recruits a following.[338] Online, distinctly different groups that share similar ideologies (white supremacists as well as anti-Semitic and anti-immigrant groups) "have begun to converge in a mutually beneficial relationship."[339] As a result, the outright bigotry or political extremism that typically exists only on the fringes of society has entered the mainstream. Klein argues that "the transitional journey, from traditional to new media, does not merely reflect a flow of followers from one venue into the next, but

---

[335] Klein.

[336] Klein, 428.

[337] George Hawley, *Right-Wing Critics of American Conservatism* (Lawrence: University Press of Kansas, 2016), 260.

[338] Klein, "Slipping Racism into the Mainstream," 428.

[339] Klein, 428.

much more so a transformative process that is changing the perception of racism, itself, through the Internet."[340]

Rather than focusing specifically on content, as many past researchers have, Klein proposed an internet-specific theory that he dubbed "information laundering," which "illustrates how 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."[341] He argues that the internet presents an "ideal counterculture environment" that allows extremist rhetoric like hate speech to thrive. Klein built the model around "four crucial domains of the web—search engines, social networks, news sites, and the blogosphere" and demonstrated how hateful rhetoric can, through information laundering, be introduced into mainstream communities online.[342] Klein grounds his theory primarily in the work of "white propaganda" (introduced by Jowett and O'Donnell) and "academic/technical ethos" (introduced by Borrowman), which he asserts offer a new way of looking at propaganda in the information age.[343] He argues that through interconnected search engines, news and research sites, political blogs, and social networks, racist rhetoric is entered as legitimate information into mainstream dialogue, even though the content itself originated from racist websites.[344] This model of information flow, which I call the Information Laundering 1.0 model, is illustrated in Figure 2. Klein provides several examples of recent mainstream conversations, including the Obama birther movement and holocaust denial, and how these discussions actually originated from racist online forums.[345]

---

[340] Klein, 431.

[341] Klein, 429.

[342] Klein, 429.

[343] Borrowman, "Critical Surfing"; Klein, "Slipping Racism into the Mainstream"; Jowett and O'Donnell, *Propaganda & Persuasion*.

[344] Borrowman, "Critical Surfing"; Klein, "Slipping Racism into the Mainstream"; Jowett and O'Donnell, *Propaganda & Persuasion*.

[345] Klein, "Slipping Racism into the Mainstream," 429.

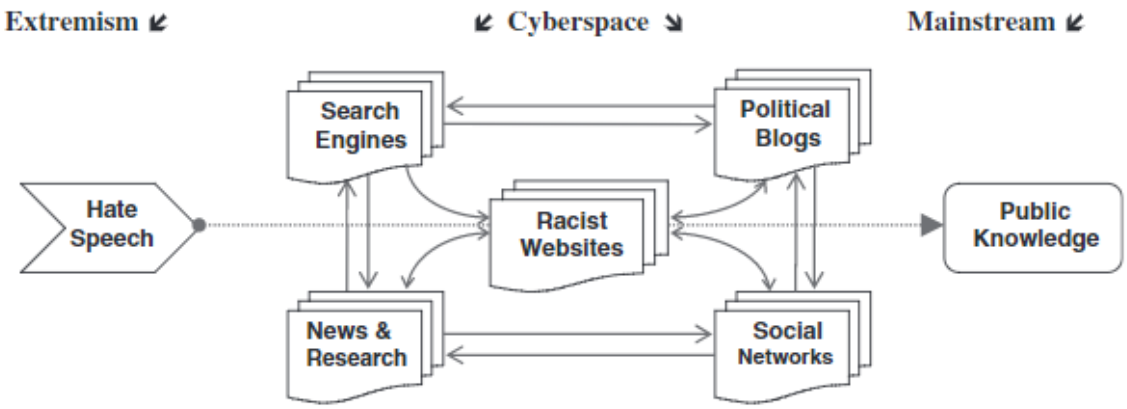

Figure 2. Information Laundering 1.0 Model[346]

While extremist racist groups may have been some of the first to take advantage of the new internet ecosystem (or perhaps simply the easiest to identify), they are not the only ones who see the value and power in this system. As a general theory, the information laundering model can help explain why the overarching online ecosystem is able to so effectively impact public discourse about many topics. If we focus on other areas of public conversation, especially truth in general, the model provides a much more powerful solution for addressing the growing rates of disinformation campaigns online. Klein argues that racist movements may have tapped into "the new wave of online politics, blogs, search engines, and social networks, in order to build the greater illusion of legitimacy and conventional support for their causes."[347] I argue that so, too, have a number of other groups, including but not limited to fake news mongers and conspiracy theorists.

The Information Laundering 1.0 model must therefore be expanded to include not only hate speech, but also other forms of misinformation, disinformation, conspiracy theories, and fake news considered together as counterfeit narratives. Further, Information Laundering 1.0 does not incorporate some of the new and emerging technology discussed in Chapter III (computational propaganda, echo chambers, and online advertising) that make this process more effective, nor does it consider secondary actors who amplify

[346] Source: Klein, 435.

[347] Klein, 431.

existing narratives in an attempt to destabilize our country or simply to make money. Although the process itself is important, the messaging's content still plays a role in the laundering process, and should therefore also be addressed within a holistic model. With these stipulations in mind, this chapter proposes the Information Laundering 2.0 model, which incorporates additional types of disinformation, as well as the technological advances that make it even more effective, and considers both amplifying actors and the content of the information being distributed.

B. INFORMATION LAUNDERING 2.0 MODEL

Like Information Laundering 1.0, Information Laundering 2.0 is built on a metaphor of money laundering. This is important because the basic principles underlying financial investigations dictate that, regardless of the type of crime, the methodology for performing the financial investigation should be the same.[348] This same structured methodology concept can be applied to information laundering, offering military officials, law enforcement, policymakers, and even the general public a way to capture and understand what is happening. However, unlike the previous model, the new model takes the metaphor a step further, incorporating all three phases of money laundering: placement, layering, and integration. Like the original model, the new model still incorporates four domains through which laundered information can be passed (discovery, information, opinion, expression); however, the new model expands opinion beyond simply "political blogs" and expression to social networks, online shopping, and gaming.

Before describing the Information Laundering 2.0 model in detail, it is important to clarify what we mean when we say "laundering." Although there are many ways to describe money laundering, the simplest way is: a process by which one can turn "'dirty' money into 'clean' money."[349] Information laundering can, likewise, be defined very simply: the process of normalizing false or extremely biased information into mainstream discourse. The FBI explains that "money laundering allows criminals to hide and

[348] U.S. Department of Justice, "Participant Guide—Basic Financial Investigations Seminar" (seminar, U.S. Department of Justice, 2013), 6.

[349] "Combating the Growing Money Laundering Threat," Federal Bureau of Investigation (FBI), October 24, 2016, https://www.fbi.gov/news/stories/combating-the-growing-money-laundering-threat.

accumulate wealth, avoid prosecution, evade taxes, increase profits through reinvestment, and fund criminal activity."[350] In this same vein of thought, information laundering allows propagandists the ability to hide and accumulate brainwashed followers, avoid prosecution, evade laws, increase cognitive capital, and legitimize subversive causes.

Information Laundering 2.0 is broken into three phases (shown in Figure 3). First is the placement phase, which prepares the information (in the form of a counterfeit narrative) for maximum impact before it is placed into the internet ecosystem. Next is the layering phase, in which the narrative is laundered through a series of domains and connections until it has reached a virality and veracity that opens it up for public discourse without the original source or motive being understood. During the layering phase, the propagandist may take advantage of accelerators—such as online advertising, computational propaganda, and echo chambers—in an effort to speed up the impact of the process. Finally, amplifiers, or actors who enhance the campaigns of other information launderers for either ideological or financial purposes, may also come into play. Upon successful laundering, the narrative enters the integration phase, where it becomes part of public discourse and knowledge.

[350] "Money laundering is the process of making illegally-gained proceeds (i.e., 'dirty money') appear legal (i.e., 'clean'). Typically, it involves three steps: placement, layering, and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the 'dirty money' appears 'clean.'" FBI, "Combating the Growing Money Laundering Threat"; see also "History of Anti-money Laundering Laws," FinCEN, accessed October 14, 2017, https://www.fincen.gov/history-anti-money-laundering-laws.

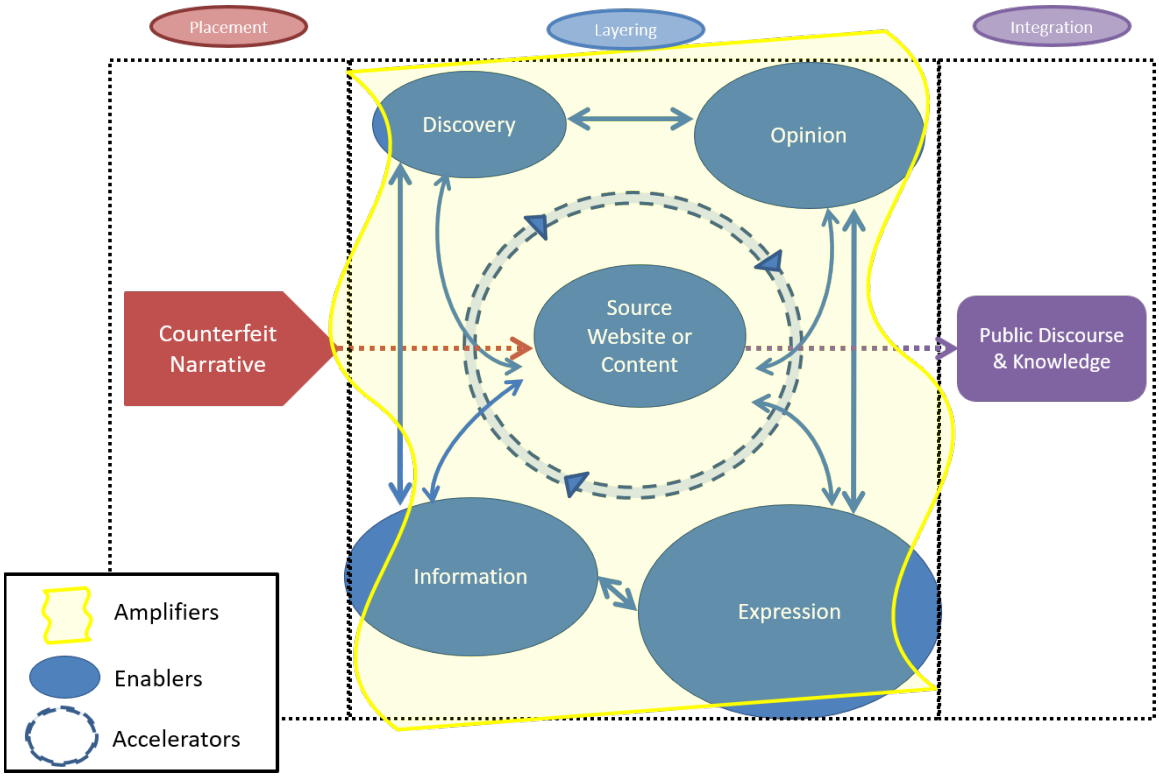

Figure 3. Information Laundering 2.0 Model

1. Placement

During the placement phase of the money laundering process, criminals prepare their "dirty money" for the layering phase (the financial system). Likewise, for information laundering, an actor must "counterfeit" his or her narrative to achieve maximum speed and virality. Part of this means exploring the audience's biases and other cognitive factors that will ensure the counterfeit narrative achieves maximum effect once it enters the internet ecosystem (the information laundering "financial system").

This is where the narrative's persuasive power—including its ethos (both academic and technical), pathos, and logos—comes into play. In the placement phase, the actor must consider the content of his or her narrative as well as the target audience to determine which message will have the greatest impact. Some research suggests that false information may be more likely to spread online than truthful information. In 2018, researchers at MIT studied Twitter posts between 2006 and 2017 to determine if the truthfulness of the tweeted information affected its spreadability. They found that "falsehood diffused significantly

farther, faster, deeper, and more broadly than the truth in all categories of information."[351] Further, false political news was the overall deepest, broadest, and most viral category. The researchers discovered that false news was spread usually by newer, less active accounts with far fewer followers, and which were typically not verified. They suggest that the novelty of false information may be the reason it travels faster through Twitter.[352]

The information launderer may even take illegal or illegitimate steps to make his or her content appear more realistic. For example, Digital Shadows, a digital risk management firm, suggests two paths through which propagandists can spread disinformation. They either 1) create content that appears legitimate by mimicking legitimate sources, or 2) compromise and take over a legitimate account.[353] Some examples of techniques used during the placement process can include:

- **Site impersonation and domain spoofing:** The actor creates a false website that mimics a legitimate website, and creates web domains that are very similar to legitimate ones.[354] There are online tools that help make the creation of false websites easier and more effective.[355] A well-developed impersonated site with a misleading domain can easily trick even savvy internet users into believing or recirculating content from these illegitimate sources.

- **Fraudulent and modified documents:** As with site impersonation, actors can create documents that appear, but are not, legitimate (fraudulent documents), or can modify the content of legitimate documents (modified documents).[356]

---

[351] Vosoughi and Aral, "The Spread of True and False News Online," 2.

[352] Vosoughi and Aral, 4.

[353] Digital Shadows, "The Business of Disinformation," 5.

[354] Digital Shadows, 5.

[355] Digital Shadows, 5.

[356] Digital Shadows, 4.

- **Account takeover:** Bad actors can leverage malicious cyber tools, often exploiting weak passwords or vulnerable credentials to take over the accounts of legitimate parties.[357] In these cases, the actors are actually modifying the legitimate source, which increases the likelihood that individuals will believe the information.

ISIS, which employs a sophisticated propaganda strategy, has leveraged many of these techniques.[358] Scott Jasper, a retired U.S. Navy captain and lecturer at the Naval Postgraduate School, and Scott Moreland, program manager for multinational exercises at the Naval Postgraduate school, explain that ISIS produces professional propaganda films to "paint their fighters as heroes."[359] They then employ these sophisticated campaigns, often hacking the social media accounts of influential users (such as U.S. Central Command) to spread their propaganda.[360]

Finally, emerging technologies, such as the audio and video editing tools discussed in Chapter III, increase the likelihood that we will see edited events, or events that never actually happened, being shared across the social web. Apart from obvious concerns, such as identity theft, the ability for an actor to create illegitimate content that looks or sounds legitimate also creates new and difficult challenges related to trust in government, journalism, and truth.

2. Layering

It can be difficult to understand the online ecosystem because it is complex—it is not formed or changed linearly. As Jose van Dijck describes it:

> We can only gain insight into the mutual shaping of platforms and apps if we view them as part of a larger online structure where every single tweak affects another part of the system. Or, to put it more general terms, the

---

[357] Digital Shadows, 4.

[358] James P. Farwell, "The Media Strategy of ISIS," *Survival* 56, no. 6 (November 2014): 49.

[359] Scott Jasper and Scott Moreland, "ISIS: An Adaptive Hybrid Threat in Transition," *Small Wars Journal*, October 29, 2016, https://calhoun.nps.edu/bitstream/handle/10945/50642/Jasper_Moreland_ISIS_%20An_Adaptive_Hybrid%20Threat_2016-10-29.pdf?sequence=1.

[360] Jasper and Moreland.

> online ecosystem is embedded in a larger sociocultural and political–economic context where it is inevitably molded by historical circumstances.[361]

Within the internet ecosystem, legitimate sources can achieve information virality and popularity by leveraging online mechanisms to spread information. In fact, many legitimate grassroots movements, such as the Arab Spring, have leveraged the ecosystem to promote awareness around the world and provide information to participants.[362] However, propagandists who deploy counterfeit narratives into the internet ecosystem can also achieve the same popularity, but through illegitimate means.

For the purposes of the information laundering model, enablers are a theoretical representation of certain aspects of the internet. Since new sites, platforms, and media are popping up all the time, enablers cannot be an all-encompassing list of every relevant influencer. To understand the model, however, it is also important to understand the concepts they represent: discovery (search engines), information (news and research), opinion (blogs and discussion forums), and expression (social networks, gaming, and online shopping). None of the enablers are completely independent. For example, at times, news and research blends into blogs and discussion forums, while also being shared and discussed via blogs and on social networks. Despite overlaps, the breakdown helps explain the information flow. As Klein explains, this layered system offers a "legitimizing factor of an interconnected information superhighway of web directories, research engines, news outlets, and social networks that collectively funnel into and out of today's hate websites."[363] The same is true for effective terrorist, extremist, and even corporate propaganda.

Accelerators also function within this ecosystem. Accelerators are tools that online propagandists leverage to accelerate their campaigns, but which are not inherently necessary to the information laundering process. For example, an accelerator can be a

---

[361] van Dijck, *Culture of Connectivity*, 9.

[362] Heather Brown, Emily Guskin, and Amy Mitchell, "The Role of Social Media in the Arab Uprisings," Pew Research Center, November 28, 2012, http://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/.

[363] Klein, "Slipping Racism into the Mainstream," 433.

technology or process that is actively or passively applied to an enabler in order to increase the effectiveness of its connection. Echo chambers are an example of a passive accelerator, while active accelerators include online advertising and computational propaganda.[364] Once a propagandist prepares the counterfeit narrative, he or she can use a combination of enablers and accelerators to push content through the ecosystem. Finally, secondary actors driven by ideological or financial motivations may also seek to amplify the effects of a propaganda campaign. These actors, referred to as amplifiers, whether working collaboratively with or independent of the primary actor, can further increase the reach of a counterfeit narrative.

a. Enablers

Because the internet's complexities continue to evolve, the information laundering process is best considered through a general understanding of online categories, rather than an understanding that focuses on a single platform. These theoretical domains, referred to as enablers, allow us to visualize the interconnectedness of the internet and the virality witch which information is spread. As with Information Laundering 1.0, enablers in Information Laundering 2.0 are broken into four categories: *discovery* (search engines), *information* (news and research), *opinion* (blogs and discussion forums), and *expression* (social networks, online shopping, and gaming).

It is important to note that several platforms are fluid and move between the various categories. Discord, for example, is a free voice and text chat service typically leveraged by gamers.[365] While this service seems applicable to *expression*, it may also, through created audio content, fit into *opinion* as well. Reddit and 4Chan also similarly blur the lines between enablers. Wikipedia, the online crowd-sourced encyclopedia, overlaps between *information* and *opinion*. Finally, YouTube, full of user-generated content and videos (*opinion* and *expression)* also plays clips and segments from mainstream media sources as well (*information)*. It is thus important to understand that these domains are fluid

[364] This is certainly not an all-encompassing list of accelerators, and new accelerators may have yet to be developed.

[365] Discord, accessed March 10, 2018, https://discordapp.com/.

and interconnected, which makes it all the more worrisome when one or more are bombarded by propaganda. The following paragraphs describe the various enablers and how each impacts both the internet ecosystem and the information laundering process.

The first enabler is *discovery*, which primarily manifests through search engines. Search engines offer a gateway to content, and this content can lead to related content, which can lead to further related content, and so on. In Information Laundering 1.0, Klein explains: "Within many of these initial hits, one finds links to other racist websites even more virulent than the first, thereby threading together in just one or two moves the radical fringe elements of cyberspace to a mainstream search engine."[366]

In 2017, the top online search engines were Google, Bing, Baidu, Yahoo, and Ask.[367] Google is the most widely used browser by far, holding more than three-quarters of the market share.[368] Search engine algorithms can (and have) prioritized hateful, extremist, or fake news if the algorithms deem them "popular" or "fresh." These algorithms assume that the more popular the site is, the more likely it will appeal to a mass audience; the algorithm is therefore more likely to assume that the information is relevant to a large number of users.[369] Freshness, or how recent and relevant the information contained on the website is believed to be, may also impact a website's ranking within the results page. Also, as mentioned in Chapter III, many search engines use customized results tailored to what they believe is of interest to that particular user. Other factors, such as the "website's location with regard to the user's server, the breadth of the query itself (the scope of information sought), existing business agreements between search engines and websites, and other emerging factors" exist.[370] All of these factors can intentionally or unintentionally bring counterfeit narratives to the top of someone's search results.

---

[366] Klein, "Slipping Racism into the Mainstream," 437.

[367] Christopher Ratcliff et al., "What Are the Top 10 Most Popular Search Engines?," Search Enginge Watch, August 8, 2016, https://searchenginewatch.com/2016/08/08/what-are-the-top-10-most-popular-search-engines/; Search Engine Market Share, accessed October 17, 2017, http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0.

[368] Ratcliff et al., "Top 10 Search Engines."

[369] Klein, "Slipping Racism into the Mainstream," 436.

[370] Klein, 436.

In Information Laundering 1.0, Klein discusses this concept through rudimentary research conducted using the keywords "white people," "black people," "Holocaust," and "Islam" on Google, Yahoo, Bing, and Ask, the top four most popular search engines at the time of Klein's research.[371] In each case he identified a website on the first page of the results that was linked to derogatory or non-factual information.[372] While the algorithms employed today are likely not the same as those employed in 2012, the fact that Google and other search engines have built algorithms that tailor search results to the user's preferences, past actions, and activity means that what one person sees in search results may be very different than what another person sees. Further, misinformation in web search engines is still rampant, especially for quickly evolving, ongoing situations such as natural disasters or crisis events. The internet is a constant, ever-evolving content landscape, and search engine algorithms are not necessarily going to adapt to emerging situations.

For example, in the wake of the Las Vegas shooting in October 2017, false reports on a 4chan thread labeled an innocent man who was unaffiliated with the incident as a "dangerous leftist" and claimed he was the shooter.[373] The subject was targeted simply because he was Facebook friends with an individual who had the same name as a person of interest in the case.[374] Nonetheless, if someone had searched for this false suspect's name in the earlier hours of the shooting, the 4chan thread would have popped up as the first result. Several more fabricated articles and links began to pop up regarding the subject as well, and a user had to scroll through as many as eight search results before reaching one that actually accurately debunked the claim.[375]

---

[371] Klein, 436.

[372] Klein, 436.

[373] Brianna Provenzano, "Facebook and Google's Algorithms Prioritized Fake News in the Wake of Las Vegas Shooting," Mic Network, October 2, 2017, https://mic.com/articles/184919/facebook-and-googles-algorithms-prioritized-fake-news-in-the-wake-of-las-vegas-shooting.

[374] Provenzano.

[375] Abby Ohlheiser and Abby Ohlheiser, "Analysis," *Washington Post*, October 2, 2017, www.washingtonpost.com/news/the-intersect/wp/2017/10/02/how-far-right-trolls-named-the-wrong-man-as-the-las-vegas-shooter/.

In another example, Google had to alter its autocomplete suggestions after the company was informed of its sexist, racist, and anti-Semitic suggestions.[376] The autocomplete feature uses an algorithm, created by Google, to offer search term suggestions based on common searches related to a partially entered topic.[377] For example, users who type the words "are Jews," "are women," or "are Muslims" into the Google search bar, were given suggested autocomplete options of "evil" and "bad."[378] Google responded to these reports by editing the autocomplete suggestions and stating:

> Autocomplete predictions are algorithmically generated based on users' search activity and interests. Users search for such a wide range of material on the web—15% of searches we see every day are new. Because of this, terms that appear in autocomplete may be unexpected or unpleasant. We do our best to prevent offensive terms, like porn and hate speech, from appearing, but we acknowledge that autocomplete isn't an exact science and we're always working to improve our algorithms.[379]

This was not the first time such an event occurred, nor will it be the last. Despite media coverage and a myriad of examples, it appears that, at least for the foreseeable future, the autocomplete feature will continue to direct users to fake content, even if they are not looking for it.[380] At least for now, when the popularity and freshness of false content is greater than that of factual reporting, the algorithm will direct people to websites that promote counterfeit narratives.

---

[376] Samuel Gibbs, "Google Alters Search Autocomplete to Remove 'Are Jews Evil' Suggestion," *Guardian*, December 5, 2016, http://www.theguardian.com/technology/2016/dec/05/google-alters-search-autocomplete-remove-are-jews-evil-suggestion.

[377] Carole Cadwalladr, "Google, Democracy and the Truth about Internet Search," *Guardian*, December 4, 2016, http://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook; Gibbs, "Google Alters Search Autocomplete"; Olivia Solon and Sam Levin, "How Google's Search Algorithm Spreads False Information with a Rightwing Bias," *Guardian*, December 16, 2016, http://www.theguardian.com/technology/2016/dec/16/google-autocomplete-rightwing-bias-algorithm-political-propaganda.

[378] Gibbs, "Google Alters Search Autocomplete."

[379] Hannah Roberts, "How Google's 'Autocomplete' Search Results Spread Fake News around the Web," *Business Insider*, December 5, 2016, http://www.businessinsider.com/autocomplete-feature-influenced-by-fake-news-stories-misleads-users-2016-12; Gibbs, "Google Alters Search Autocomplete to Remove 'Are Jews Evil' Suggestion."

[380] Roberts, "Google's Autocomplete."

Information, through news and research, is the second internet ecosystem enabler that propagandists leverage to launder counterfeit narratives. The Pew Research Center, a nonpartisan American think tank, along with other leading research organizations, has been tracking and defining the role the internet plays in the consumption of information and news. Journalism has been particularly motivated to understand this phenomenon, as the internet, through its free and continuous flow of information, has also significantly impacted the survival of traditional media platforms such as newspapers, magazines, and television, the effects of which are still being realized.[381] Mainstream news outlets are no longer the gatekeepers of information; as a result, a number of other news, pseudo-news, and flat-out false news sites have made their way into mainstream culture. Alternative media sources have also popped up in recent years, some of which may claim they are helping to minimize extremist ideology by wrapping it in mainstream, accepted ideas.[382]

Additionally, a large number of people leverage social media platforms such as Twitter and Facebook as a primary source of news. In 2013, 2016, and 2017, the Pew Research Center produced reports called *News Use across Social Media Platforms*, which analyze the scope, characteristics, and trends related to media consumption online.[383] The 2017 report concluded that two-thirds of adults in the United States get some or all of their news from social media platforms.[384] The *Reuters Digital News Report 2017* found that

---

[381] Jeffrey Dvorkin, "Column: Why Click-Bait Will Be the Death of Journalism," PBS NewsHour, 2016, http://www.pbs.org/newshour/making-sense/what-you-dont-know-about-click-bait-journalism-could-kill-you/; Kimmo Lundén, "The Death of Print? The Challenges and Opportunities Facing the Print Media on the Web" (fellowship paper, University of Oxford, 2008), http://reutersinstitute.politics.ox.ac.uk/sites/default/files/The%20Death%20of%20Print%20-%20The%20Challenges%20and%20Opportunities%20facing%20the%20Print%20Media%20on%20the%20Web.pdf.

[382] "For more than a year, Yiannopoulos led the site in a coy dance around the movement's nastier edges, writing stories that minimized the role of neo-Nazis and white nationalists while giving its politer voices 'a fair hearing.'" Joseph Bernstein, "Here's How Breitbart and Milo Smuggled Nazi and White Nationalist Ideas into the Mainstream," BuzzFeed, accessed October 15, 2017, https://www.buzzfeed.com/josephbernstein/heres-how-breitbart-and-milo-smuggled-white-nationalism.

[383] Jesse Holcomb, Jeffrey Gottfried, and Amy Mitchell, "News Use across Social Media Platforms," Pew Research Center, November 14, 2013, http://www.journalism.org/2013/11/14/news-use-across-social-media-platforms/; Jeffrey Gottfried and Elisa Shearer, "News Use across Social Media Platforms 2016," Pew Research Center, May 26, 2016, http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/; Elisa Shearer and Jeffrey Gottfried, "News Use across Social Media Platforms 2017," Pew Research Center, September 7, 2017, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

[384] Shearer and Gottfried, "News Use 2017," 2.

fifty-one percent of its U.S. sample received its news from social media.[385] However, Reuters noted that only 2 percent of those polled used *only* social media to view the news; most used a combination of different platforms and sources.[386]

Further, extremist groups have formed their own think tanks and research organizations; nation-states are masquerading as legitimate scholarly sources; and big business is funding and manipulating research to fit their marketing needs. For example, the Institute for Historical Review uses legitimate-sounding titles, credentials, and scholarly signifiers, such as Ph.D., to portray an air of mainstream authenticity to visitors, when in fact they are a holocaust denier propaganda platform.[387] The National Policy Institute (NPI), the white nationalist think tank run by Richard Spencer that spawned the "alt-right," also masquerades as a legitimate think tank.[388] NPI publishes research and books and boasts a mission statement that the organization is "dedicated to the heritage, identity, and future of people of European descent in the United States, and around the world."[389] NPI even has annual conferences. During the notable 2017 conference, a number of members in the audience gave a Nazi salute following Spencer's address.[390] NPI, as *Wired* magazine describes it, packages its "most controversial ideas in pseudo-academic arguments, using ornate, polysyllabic, radical slur–free language."[391]

---

385 Nic Newman et al., *Reuters Institute Digital News Report 2017* (Oxford: Reuters Institute, 2017), 10, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf?utm_source=digitalnewsreport.org&utm_medium=referral.

386 Newman et al., 10.

387 Klein, "Slipping Racism into the Mainstream," 438.

388 Emma Grey Ellis et al., "How the Alt-Right Grew from an Obscure Racist Cabal," *Wired*, October 9, 2016, https://www.wired.com/2016/10/alt-right-grew-obscure-racist-cabal/.

389 Ellis et al.

390 Daniel Lombroso and Yoni Appelbaum, "'Hail Trump!': Video of White Nationalists Cheering the President-Elect," *The Atlantic*, November 21, 2016, http://www.theatlantic.com/politics/archive/2016/11/richard-spencer-speech-npi/508379/.

391 Ellis et al., "Alt-Right."

These extremist groups also leverage popular platform layouts and features, like those on Wikipedia, for example, to create their own "alternative" sites such as Metapedia.com.[392] Metapedia looks and feels like Wikipedia, but houses information and rhetoric related to the white nationalist movement.[393] At first glance, Metapedia does not appear to reflect racist ideals. The site offers that it "is an electronic encyclopedia which focuses on culture, art, science, philosophy and politics."[394] However, upon closer examination, white supremacist rhetoric is wrapped within the text.

Additionally, research funded and then manipulated by big business may also contribute to the distrust of information and the general public's susceptibility to misinformation. From the tobacco industry to the automotive industry, companies are identifying or specifically funding research that benefits their bottom line.[395] Further, corporate propagandists may employ techniques such as selective sharing—identifying factual or science-based information that supports the preferred industry position, and then sharing *only* that information, even when counterpoints to that information exist.[396] An industry may also fund and support research that could be used to counter research from the scientific community, a process known as biased production.[397] While these issues are not necessarily information laundering of counterfeit narratives, they certainly, when brought to light, call into question the trustworthiness of big business and corporations.

Beyond the more structured domains of search engines and news and research comes the third enabler, *opinion*. This enabler incorporates the blogosphere and other discussion forums. These are the platforms and services that engage in a high amount of

---

[392] Klein, "Slipping Racism into the Mainstream," 437.

[393] Klein, 437.

[394] "Main Page," Metapedia, accessed February 10, 2018, https://webcache.googleusercontent.com/search?q=cache:7asnJsdEV58J:en.metapedia.org/wiki/Main_Page+&cd=1&hl=en&ct=clnk&gl=us.

[395] Jack Ewing, "10 Monkeys and a Beetle: Inside VW's Campaign for 'Clean Diesel,'" *New York Times*, January 25, 2018, https://www.nytimes.com/2018/01/25/world/europe/volkswagen-diesel-emissions-monkeys.html; James Owen Weatherall, Cailin O'Connor, and Justin Bruner, "How to Beat Science and Influence People: Policy Makers and Propaganda in Epistemic Networks," Cornell University Library, January 4, 2018, 4, http://arxiv.org/abs/1801.01239.

[396] Weatherall, O'Connor, and Bruner, "How to Beat Science and Influence People," 2.

[397] Weatherall, O'Connor, and Bruner, 4.

"user-generated content" and "support creativity, foreground cultural activity, and promote the exchange of amateur or professional content."[398] YouTube, Medium, Reddit, and 4chan all play a role in the spread, discussion, and influence of information, especially information that is new and emerging, or which contradicts the framing and dialogue being presented by authority figures.[399] This realm is what Klein describes as "unrestrained civic discourse."[400] The blogosphere is "far more concerned with the opinions of everyday people than with the facts and drawn conclusions of experts and reporters."[401] Often, as was the case in Pizzagate and many of the conspiracy theories associated with critical incidents, this enabler is the original source for the content or is the location where a link to an extremist or false website is posted and discussed.

Finally, the fourth enabler, and the one garnering the majority of the attention in light of the 2016 presidential election, is *expression*. Expression incorporates social networks, online shopping, and gaming. Here, platforms offer "dynamic spaces were individual and cultural identities are expressed, tried on, and shared."[402] These are the traditional sites that have been dubbed "social network sites," and which "primarily promote interpersonal contact, whether between individuals or groups; they forge personal professional, or geographical connections and encourage weak ties."[403] Also included in *expression* are "trading and marketing sites," which are primarily used to exchange or sell goods and services.[404] Amazon, eBay, Craigslist, and Backpage fall into this category. Finally, "play and game sites," which incorporate communities such as Twitch, Steam, and other single or multiplayer online games that have some sort of chat-based component are also considered *expression*.

---

398 van Dijck, *Culture of Connectivity*, 8.

399 See www.youtube.com; https://medium.com; www.4chan.org; www.reddit.com.

400 Klein, "Slipping Racism into the Mainstream," 439.

401 Klein, 439.

402 Klein, 441.

403 van Dijck, *Culture of Connectivity*, 8.

404 van Dijck, 8.

b. Accelerators

In 2017, Freedom House reported that governments have been increasingly attempting to control online communications in their countries. They noted that, since 2009, tradecraft has become increasingly sophisticated, "with bots, propaganda producers, and fake news outlets exploiting social media and search algorithms to ensure high visibility and seamless integration with trusted content."[405] The exploitation of online mechanisms such as echo chambers, advertising, and computational propaganda, referred to in this model as accelerators, have made information laundering more effective, more efficient, and in many cases more profitable. Accelerators are not required for information laundering to occur, but they can speed up the process. For example, the 2018 MIT study about the spread of true and false news on Twitter mentioned bot technology, finding that, although bot use has "accelerated the spread of both true and false news, it affected their spread roughly equally."[406] Because the study concluded that false news travels more rapidly online than true news, this implies that humans play a crucial role in the rapid sharing of false information. Nonetheless, if the information launderer employs bots, he or she can certainly spread a counterfeit narrative more rapidly.

Accelerators can be broken down into categories: passive accelerators and active accelerators. Passive accelerators, such as echo chambers, are mechanisms of the ecosystem that enhance the spread of counterfeit narratives, and that are not directly dependent upon the launderer's actions. While these mechanisms do enhance the laundering effect, the launderer does not need to purposefully enact them; they occur on their own. Active accelerators, like computational propaganda and online advertising, however, require purposeful enactment by the launderer.

---

[405] Freedom House, "Manipulating Social Media," 2.

[406] Vosoughi and Aral, "The Spread of True and False News Online," 5.

c. Amplifiers

As we attempt to quantity the effectiveness of counterfeit narratives, we must consider the potential motivations of the facilitating actors. If we understand the actors, we may be able to anticipate their next moves and develop counter-methods to undermine their disinformation efforts. In doing so, we must also consider secondary actors who might leverage counterfeit narratives for their own ideological or financial benefit. These secondary actors, referred to as amplifiers in the Information Laundering 2.0 model, do not create their own disinformation campaigns, but seek to exploit existing unrest or confusion created by primary actors. They thus amplify the primary actor's efforts. When considering Jowett and O'Donnell's categories of propaganda, amplifiers likely engage in black propaganda because they intentionally mislead or conceal their source to increase the likelihood that the message will seem credible. There are two types of amplifiers: ideologically motivated amplifiers and financially motivated amplifiers.

Ideologically motivated amplifiers are secondary actors who take advantage of one or several existing information laundering campaigns to create confusion, sow discord, and undermine democracy. When these actors are nation-states, their tactics are often considered hybrid warfare. Russia, one of the nation-states accused of leveraging hybrid warfare tactics against the United States and other countries, has garnered much attention. A number of scholars, government agencies, think tanks, and military officials are attempting to understand the impact Russian hybrid warfare tactics have on America's democracy. Information warfare, a subset of hybrid warfare, has been an area of particular concern. In his testimony to the United States House of Representatives Committee on Armed Services on March 22, 2017, RAND political scientist Christopher Chivvis explained the role information warfare plays in Russia's larger hybrid warfare strategy:

> The objective of these information operations is primarily to muddy the waters and cast doubt upon objective truths. Needless to say, these media outlets do not share established Western journalistic practices regarding factual evidence and truth. They aim to shape the political discussion in ways that will benefit the Kremlin.[407]

In 2016, RAND researchers Christopher Paul and Miriam Matthews identified four distinct features of Russia's contemporary propaganda effort: it is 1) "high-volume and multichannel," 2) "rapid, continuous, and repetitive," 3) it "lacks commitment to objective reality," and 4) it "lacks commitment to consistency."[408]

Nation-states may be in the best position to take advantage of existing counterfeit narratives and information laundering. Researchers argue that when counterfeit narratives are effectively employed, they can undermine or disrupt our government and society so completely that it can allow an adversary to achieve its political and military goals without armed combat.[409] In the testimonial words of Kevin Mandia, chief executive officer of FireEye (a leading security technologies company), "if all our tools worked against them and all their tools worked against us, in cyberspace, Russia wins … cyber on cyber, just feels like we're in a glass house throwing rocks at a mud hut."[410]

According to the recent indictment of thirteen Russians believed to have interfered in the 2016 U.S. presidential election, the Internet Research Agency spent millions of dollars and employed hundreds of people to conduct online influence operations in an effort to sow Americans' distrust in their political system and the election process.[411] The goal was to "conduct what it called 'information warfare against the United States of America' through fictitious U.S. personas on social media platforms and other Internet-based

---

[407] Christopher S. Chivvis, *Understanding Russian 'Hybrid Warfare' and What Can Be Done about it* (Santa Monica, CA: RAND, 2017), https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

[408] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter it* (Santa Monica, CA: RAND, 2016), 2.

[409] Allenby and Garreau, "Weaponized Narrative," 6.

[410] "Russian Interference in 2016 Election, Part 2, (Testimony to Congress)," C-SPAN video, March 30, 2017, 1:34:02–1:34:40, https://www.c-span.org/video/?426227-101/senator-rubio-confirms-campaign-staff-targeted-russian-hackers.

[411] United States of America v. Internet Research Agency, 4–5.

media."[412] Internet Research Agency employees were specifically instructed to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements."[413] By 2016, many groups created by these co-conspirators on Facebook and Instagram had garnered hundreds of thousands of followers.[414] The Internet Research Agency measured the impact of its messaging and conducted content analysis to enhance the perceived authenticity of its posts.[415]

Court documents also indicate that the co-conspirators interacted with legitimate grassroots organizations involved in the 2016 election process in an effort to increase their legitimacy, spread rumors, and create discord.[416] Often, according to the documents, these individuals unwittingly re-distributed propaganda posted by Russian actors. The co-conspirators used these unwitting individuals to plan various rallies in New York, Florida, North Carolina, and Pennsylvania. The Russian actors posed as Americans and encouraged actual Americans to attend these rallies, and promoted the events via advertisements purchased on Facebook and Instagram. The co-conspirators even reached out to Americans through personal messages to request participation in the rallies, going so far as to pay Americans to attend rallies, carry signs, and dress up in costumes (for instance, dressing up as Hillary Clinton in a prison uniform).[417] Further, the court documents indicate that the Internet Research Agency purchased server space on U.S.-based infrastructure. Its employees then used stolen personal information to open PayPal accounts, obtain false driver's licenses, and post to social media accounts controlled by the Internet Research Agency posing as the victims whose identities were stolen. These actors also used the false identification to purchase online advertisements.

---

[412] United States of America v. Internet Research Agency, 6.

[413] United States of America v. Internet Research Agency, 14.

[414] United States of America v. Internet Research Agency, 14.

[415] United States of America v. Internet Research Agency, 15.

[416] United States of America v. Internet Research Agency, 13.

[417] United States of America v. Internet Research Agency, 25–27.

On the other end of the spectrum are financially motivated amplifiers, or actors who take advantage of an existing laundering campaign to make money. For example, the "fake news factory" churning out thousands of fake articles in Veles, Macedonia, is an example of a well-documented arguably nefarious actors engaging in financially motivated amplification. For financially motivated amplifiers, the goal is not to reach an ideological objective but simply to profit. However, these amplifiers may unintentionally sow chaos, disorder, and confusion as well.

3. Integration

Money laundering is a significant crime that "can undermine the integrity and stability of financial institutions and systems, discourage foreign investment, and distort international capital flows."[418] Information laundering is also a significant crime; it can undermine the integrity and stability of government, military, and educational institutions and systems, discourage foreign diplomacy, and distort international and domestic opinion. As with money laundering, propagandists can use information laundering to "anonymize" the source of the information, making it difficult for users to track where the original conversation started.

It is important to note that, while this theory applies to the internet ecosystem, media and information from outside the internet also play a role in information laundering. Information Laundering 2.0 can include the use of traditional forms of media as well as direct, first-person interaction with events (i.e., when people record or livestream an event). For example, citizens often view news broadcasts, TV shows, and other entertainment through online hosting platforms. Additionally, clips from these more traditional mediums, as well as both taped and livestreamed events in the real world, are often shared online, adding to the information laundering's complexity and effectiveness. This concept will be increasingly important when technologies that are currently being developed, as discussed in Chapter III, emerge into mainstream use.

[418] FBI, "Combating the Growing Money Laundering Threat."

THIS PAGE INTENTIONALLY LEFT BLANK

V. HOW WE SAVE THE WORLD (AND OTHER USEFUL TIPS)

Every day, new technologies and new connections are made online. Whether you are an early adopter or an all-out internet avoider, the merging of physical space and cyber space has become a nearly unavoidable evolution of humanity. Even if you do not use social media—do not tweet, do not share on Facebook, do not upload videos to YouTube—you still have an online presence. You still have a job, you still vote, you still pay taxes. And those actions are increasingly being recorded and made visible online. Even those who feel removed from the online world are still part of a system that is under attack.

As the line between the physical world and the cyber world continues to blur, the effects of online information laundering will leak increasingly into our offline world. In fact, the expanded definition of "fake news" to include any fact or topic one disagrees with may be the ultimate counterfeit narrative of them all. If you convince people that nothing is true, their desire for inaction intensifies. For example, while conspiracy theories may help people feel in more immediate control, they eventually breed mistrust, paranoia, and isolation, which can lead to incorrect action or non-action.[419] So what happens when an entire country is paralyzed by falsehoods? If we stay on course, we may soon find out.

The question then becomes: What can we do? As this thesis has proposed, the fact that false information, extremist content, and hate speech are present on the internet is not the primary issue at hand; the root of that problem is an argument over freedom of speech. We should not have to sacrifice freedom of speech for freedom of fact. The primary concern is that internet actors, malicious or otherwise, are attempting to pass false or extremely misleading information through the internet ecosystem in a manner that makes it appear factual, and to then create consensus around counterfeit narratives. To combat this threat, we must address not only the counterfeit narratives and internet ecosystem itself, but also the accelerators and amplifiers that accelerate and monetize information laundering. These issues are happening in real time; as enablers become more saturated with false content, accelerators and amplifiers also become more dynamic, robust, and

[419] Jolley and Douglas, "Social Consequences of Conspiracism."

prevalent. While many U.S. citizens realize that these disinformation campaigns are out there, most do not truly understand their potential for real harm. As Mark Goodman put it, "The problem of course is not that technology is bad but that so few understand it."[420]

Anya Schiffrin explained that strategies for combating disinformation campaigns are typically broken into supply-side strategies and demand-side strategies.[421] While both have potentially valid input for combating the threat, neither can do it alone. The problem needs to be addressed from both a supply side and a demand side, as well as holistically. To combat money laundering, "the FBI focuses its efforts on money laundering facilitation, targeting professional money launderers, key facilitators, gatekeepers, and complicit financial institutions, among others."[422] If we follow this model, the solutions—and the agencies and organizations we select to implement these solutions—should focus their efforts on information laundering facilitation, targeting professional information launderers, key facilitators, gatekeepers, and complicit technology companies.

While the Information Laundering 2.0 model does not offer a simple, step-by-step solution for combating this complex problem, it frames the issue in a way that homeland security professionals, law enforcement, policymakers, and the general public can understand it. It offers the possibility of real-world solutions leveraged at multiple levels while protecting free speech, and without sacrificing our nation's cognitive security. The Information Laundering 2.0 model should be used to address global, governmental, societal, and individual responses to this continuous threat. We must identify solutions that address the problem at every phase (placement, layering, and integration) and through every piece (enablers, accelerators, and amplifiers).

In September 2017, the Atlantic Council released a report written by Matthew Chessen, senior technology policy adviser to the Secretary of State, which offers a number of policy recommendations for this new environment of disinformation, especially

---

[420] Goodman, *Future Crimes*, 447.

[421] Schiffrin, "How Europe Fights Fake News."

[422] FBI, "Combating the Growing Money Laundering Threat."

considering the looming threat of artificial intelligence.[423] Additionally, a report released in late March 2018 by the Social Media Working Group for Emergency Services and Disaster Management (SMWGESDM)—sponsored by the Department of Homeland Security's Science and Technology Directorate—recommends a number of best practices for countering misinformation during disasters and emergencies.[424] This chapter outlines how many of Chessen's and the SMWGESDM's recommendations, as well as other potential strategies for combating this issue, can be understood and implemented through the information laundering framework.

The solutions are broken down first by explaining where they fit in the Information Laundering 2.0 model, and then the entire information laundering process is taken into consideration. This chapter also provides specific strategies for homeland security officials to consider. Any solutions or steps to combat information laundering should be discussed using a multi-level, multi-disciplinary, and multi-sector approach. This chapter is therefore not the definitive guide to ending information laundering; it is simply a place to start the conversation, start the research, and start the response.

A. PREVENT PLACEMENT OF THE COUNTERFEIT NARRATIVE INTO THE SYSTEM

In light of emerging research (such as the 2018 MIT study about the spread of false news on Twitter), preventing counterfeit narratives from entering the internet ecosystem altogether may be one of the strongest mitigation measures. The chart in Figure 4 shows where this strategy falls on the Information Laundering 2.0 model. However, it can be tricky to prevent counterfeit narratives; doing so involves both content-driven and content-neutral strategies.

---

[423] Chessen, "The MADCOM Future."

[424] The Social Media Working Group for Emergency Services and Disaster Response (SMWGESDM) was created by the U.S. Department of Homeland Security's Science and Technology Directorate (S&T). It comprises a cross-section of subject-matter experts from federal, tribal, territorial, state, and local responders. See SMWGESDM, "Countering Misinformation."

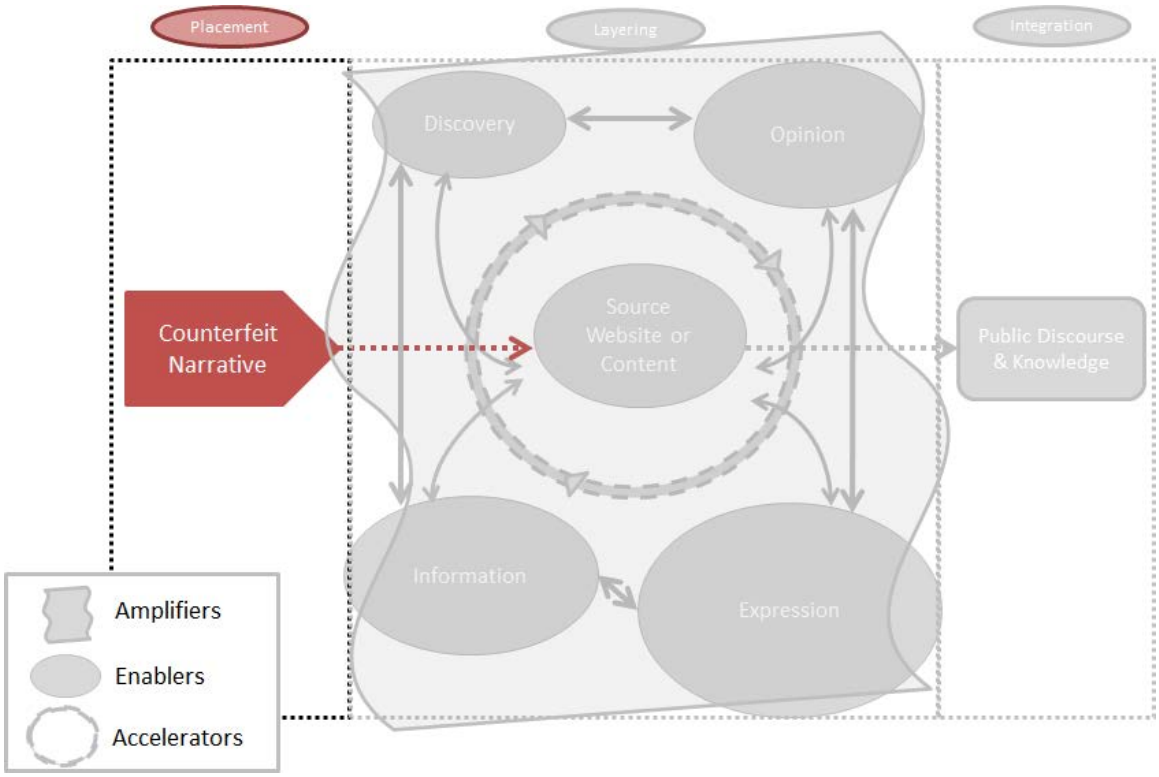

Figure 4. Preventing a Counterfeit Narrative from Entering the System

From a content-driven perspective, we can define what constitutes a counterfeit narrative, balancing the harm of the narrative with the actor's right to free speech. There is precedent for this, as steps have been made surrounding hate speech, child pornography, and threats. From a content-neutral standpoint, there are several techniques that can help limit the effectiveness of counterfeit narratives. Identifying, and understanding, the online technologies that can be used to create more impactful narratives, and then *criminalizing* the use of these technologies, could help. For example, if an actor uses a technology to create a fake tweet—meant to look like it is posted from a legitimate person's account—in an effort to undermine someone's credibility or spread fear and panic, this should be considered identity theft. There are countless examples of this practice; for instance, in April 2013, hackers broke into an Associated Press (AP) Twitter account and tweeted that

there had been an explosion at the White House and that President Barack Obama was injured.[425] The Syrian Electronic Army later took responsibility for the hoax tweet.[426]

More recently, in February 2018, *Miami Herald* Reporter Alex Harris had a similar experience during his attempt to cover the Parkland, Florida, shooting.[427] A perpetrator created two fake tweets: one requested photos of dead bodies and the other asked if the shooter was white. The tweets appeared to come from Harris's account, but actually came from a false Twitter account. Angry posts began to roll into the reporter's Twitter feed. In the Parkland, Florida, case, the reporter's account was not actually hacked or taken over. Instead, the impersonator used free online software to create authentic-looking tweets.[428] Somebody also created and disseminated a false news article, meant to look like it had come from the *Miami Herald*, which indicated that an additional mass shooting was threatened at a Miami–Dade middle school.[429] Experts claimed that this incident was especially troubling, as the "instigators hijacked the brand of the news organization and the name of respected reporters."[430]

It may therefore be beneficial to develop clear guidelines and rules governing these activities; economic regulation and civil laws, such as copyright and trademark laws, may be the place to start. For example, some online tools help propagandists impersonate existing sites, but with few legal repercussions. If an existing website were to issue a "cease and desist order," propagandists would no longer be able to legally leverage the tool.[431] Additionally, creating and enforcing truth in advertising—including political advertising—rules online may reduce the number of counterfeit narratives spread online.

---

[425] David Jackson, "AP Twitter Feed Hacked; No Attack at White House," *USA Today*, April 23, 2013, https://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/.

[426] Jackson.

[427] Tim Johnson, "Hoax Attempts against Miami Herald Augur Brewing War over Fake, Real News," McClathcy DC Bureau, February 24, 2018, http://www.mcclatchydc.com/news/nation-world/national/article201938144.html.

[428] Johnson.

[429] Johnson.

[430] Johnson.

[431] Digital Shadows, "The Business of Disinformation," 11.

We must also address the rampant parody and alias accounts on various online platforms. To do so, technology companies could develop better ways to label these accounts and work to confirm the identity of individuals who use these accounts to act in an official capacity. From a money laundering standpoint, an individual has to properly identify him or herself before using the financial system. If we can find ways to validate user accounts, or leverage existing services that do so, we can more easily attribute information to the *real* people posting it, and trace counterfeit narratives back to their true illegitimate accounts. This practice, of course, would need to be considered and balanced against an individual's right to privacy (specifically anonymity) online.

At the individual level, we can also take steps to increase cyber hygiene. Individuals should be aware of proper cybersecurity practices and account protections, including the use of strong passwords and dual authentication, if available. If the Associated Press had practiced better cyber hygiene, perhaps its account would not have been hacked and the tweet about President Obama would not have been posted. While it is, of course, important to protect ourselves against identity theft and other online criminal activity, awareness of good cyber hygiene practices also creates a barrier against our involuntary complicity in widespread, online information laundering campaigns.

From a homeland security and public safety perspective, we must also urgently consider emerging technologies such as video and audio editing—including how they spread counterfeit narratives, and how to combat them. SMWGESDM suggests that, as we wait for these technologies to develop and become more sophisticated, we can examine the use of livestream video services, like Periscope, Facebook Live, or YouTube, to correct or stop counterfeit narratives from spreading before they start.[432]

[432] SMWGESDM, "Countering Misinformation."

B. RE-LEGITIMIZE AND REINFORCE ENABLERS

Information laundering works because loose connections between various websites create a false sense of legitimacy for illegitimate websites or content. Tackling the algorithms and processes through which these connections are made, or through which linked material is vetted, could strengthen connections between vetted sources and weaken connections between un-vetted sources. The chart in Figure 5 shows where this strategy falls on the Information Laundering 2.0 model. Again, increased attribution and labeling could help. If fact-checking sites (such as mediabiasfactcheck.com, snopes.com, and politifact.com) were to clearly mark articles as opinions or advertisements, readers could more easily ascertain if the source can be trusted.

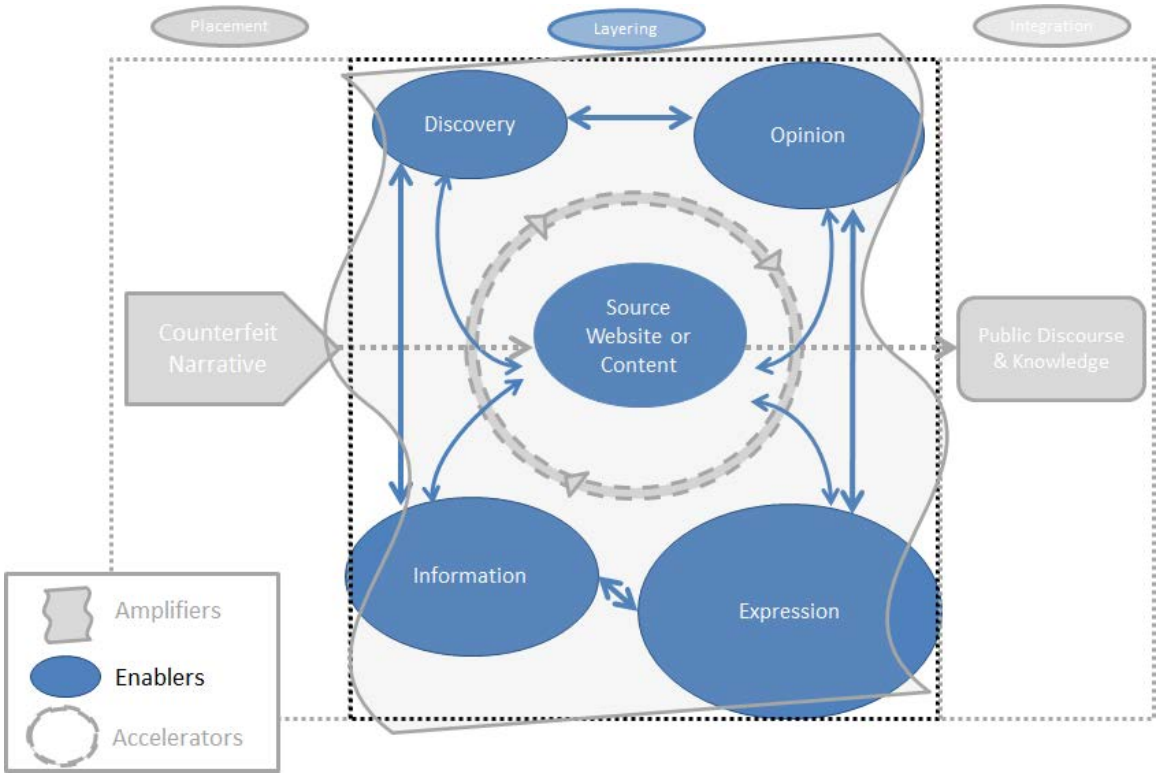

Figure 5. Re-legitimizing and Reinforcing Enablers

Further, rebuilding trust in the enablers themselves, especially in regards to *information* (news and research) and *expression* (social media), will help increase the public's trust. From a holistic approach, stronger regulations (and enforcement when those regulations are violated) should also be considered. Counterfeit narratives work because they amplify perceived injustice and sow division. Related scandals undermine the public's trust in companies, institutions, and governments: such as when Volkswagen attempted to cheat emission tests by funding manipulative research, causing deadly nitrogen oxide pollution; when government officials in Flint, Michigan, implemented cost-saving measures that tainted drinking water with lead and other toxins; and when the sugar industry paid scientists to conduct research that concluded sugar does not play a role in heart disease.[433] While these practices may not specifically point to information laundering, when trusted experts pay to get the answer they want, and then release that information to the public, the result can be just as dishonest and unethical as information laundering. When trusted experts disregard transparency, they increase the likelihood that counterfeit narratives will be developed.

C. SLOW DOWN THE ACCELERATORS

Because accelerators primarily stem from profit-driven processes created by corporations that veil their methods in secrecy, we do not yet fully understand how these tools work, how they are spreading counterfeit narratives, or how we can stop them. Academia, government, and private-sector partners should therefore work together to mitigate the impact of current and emerging accelerators. The chart in Figure 6 shows where this strategy falls on the Information Laundering 2.0 model.

[433] Ewing, "10 Monkeys and a Beetle"; Coral Davenport and Jack Ewing, "VW Is Said to Cheat on Diesel Emissions; U.S. to Order Big Recall," *New York Times*, September 18, 2015, www.nytimes.com/2015/09/19/business/volkswagen-is-ordered-to-recall-nearly-500000-vehicles-over-emissions-software.html; "Flint Water Advisory Task Force Final Report," State of Michigan, March 2016, http://www.michigan.gov/documents/snyder/FWATF_FINAL_REPORT_21March2016_517805_7.pdf; Camila Domonoske, "50 Years Ago, Sugar Industry Quietly Paid Scientists to Point Blame at Fat," NPR, September 13, 2016, https://www.npr.org/sections/thetwo-way/2016/09/13/493739074/50-years-ago-sugar-industry-quietly-paid-scientists-to-point-blame-at-fat.

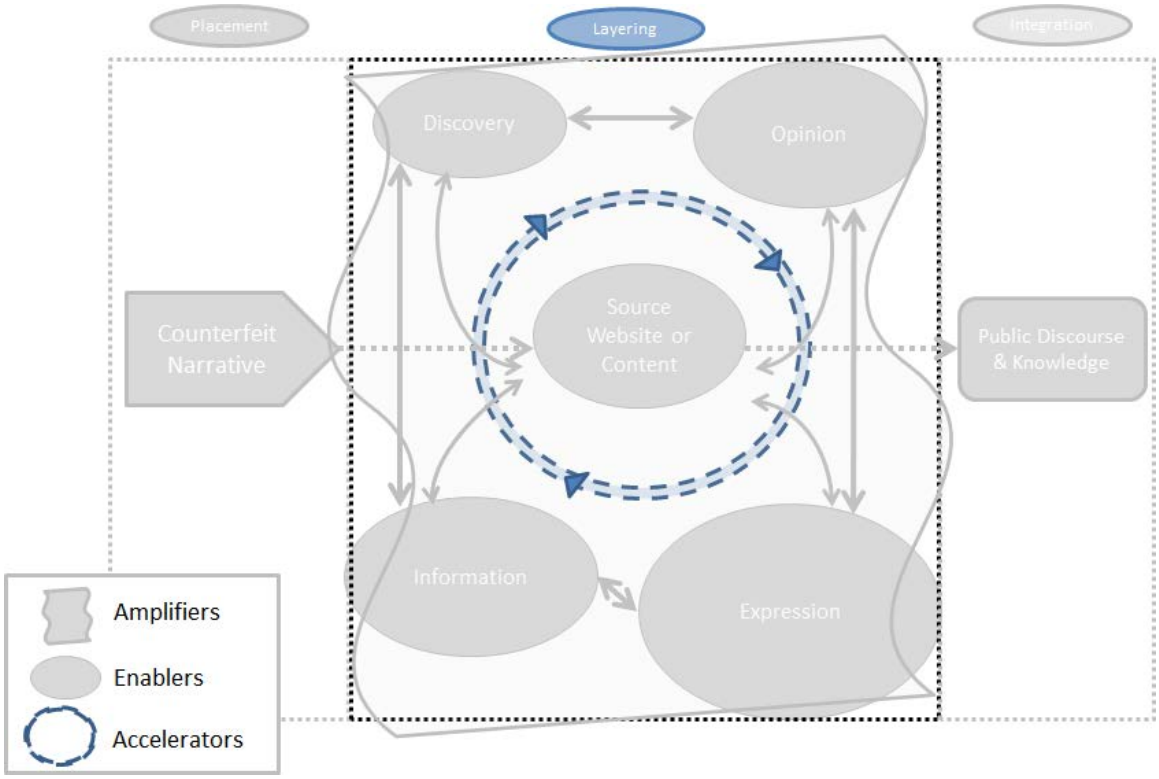

Figure 6. Slowing down the Accelerators

As we grow nearer to the adoption of true artificial intelligence and MADCOMs, researchers and policymakers must focus more attention on the biases in algorithms. Chessen suggests that technology companies should fund research that seeks to develop open-source tools for sharing incidents of fake news, disinformation, and the information laundering campaigns themselves.[434] Tristan Harris, introduced in Chapter III, offers three radical changes to technology and society that could potentially address the issue of people spending far too much time online. These solutions may also help address information laundering, especially in regards to slowing down the accelerators. First, Harris says we must acknowledge that we are persuadable and that there might be something we want to protect.[435] Second, we need new accountability system models; as information online becomes more and more persuasive, we must ensure that the people in the control rooms

[434] Chessen, "The MADCOM Future," 20.

[435] Harris, "Handful of Tech Companies," 11:01.

are transparent and accountable for the public's wants. To do this, he says, we must question big ideas, like the business model for advertising. Finally, he argues that we need a "design renaissance"—once we understand that our technology can influence the behavior of billions of people, we must ensure that influence is positive. As one technology insider proclaimed during an anonymous podcast, "Do you want to just sell me more stuff, or are you going to actually help us become better humans?"[436] To address the most vicious accelerators, bots, we may need to consider legislation. There is, in fact, some precedence for this strategy. In 2016, in an effort to ensure fairness in online ticket sales, Congress passed the Better Online Tickets Sales Act, which made it unlawful for actors to use automated bots to buy tickets online.[437]

As the information laundering model mirrors the money laundering model, the Bank Secrecy Act may also offer innovative ideas for tackling this issue. The Bank Secrecy Act which mandates specific reporting requirements related to potential money laundering activity; a similar act could afford law enforcement, investigators, and everyday citizens the ability to track information that is being laundering through the internet ecosystem. For example, banks and other financial entities are required to file a currency transaction report if an individual conducts a single-day withdrawal or deposit of more than $10,000. A currency transaction report is not indicative of criminal activity; it simply records a history of currency transaction reports that could indicate potential money laundering. If banks or other financial entities identify potential criminal activity, they can file a suspicious activity report to explain the behavior.

Similarly, thresholds for certain activity online could trigger similar reports. For example, if a given social media account sees a lot of traffic or behavior indicative of bot involvement, it could be flagged with an information laundering equivalent to a currency transaction report. If the same account exhibits signs of information laundering, a suspicious activity report could be filed. Further, additional research should be conducted

---

[436] TED, "Sad in Silicon Valley," *Sincerely, X* (podcast), August 10, 2017, https://art19.com/shows/sincerely-x/episodes/f7d7cf3f-9002-4ac2-b67c-6118fa44978e.

[437] "Better Online Ticket Sales Act of 2016," United States Code § (2016).

on the potential benefit of new technologies, such as big data, artificial intelligence, and the blockchain, that could be leveraged to help combat this issue.

D. ATTACK THE AMPLIFIERS

The Global Engagement Center of the U.S. Department of State, established in April 2016 by President Barack Obama, is the agency currently leading the government efforts to combat propaganda and disinformation from nation-states and foreign terrorist groups.[438] The Global Engagement Center was codified into law by Congress in fiscal year 2017 through the National Defense Authorization Act (NDAA). However, according to an article published by the *New York Times* on March 4, 2018, despite being granted $120 million dollars to combat Russian meddling, the State Department has not spent a dime.[439] This means that, while the Global Engagement Center exists and it can and should be used to combat Russian information warfare efforts, it is not effectively doing so.

When it comes to amplifiers, especially considering the actions of both Russia and Macedonia, we must also explore the resources and capabilities afforded by the United States Intelligence Community, which operates under Executive Order 12333. Amplifiers are foreign nations or actors who are attempting to influence operations on a domestic population; this activity could therefore fall under the Intelligence Community's purview. The chart in Figure 7 shows where this strategy falls on the Information Laundering 2.0 model.

---

438 "Global Engagement Center," U.S. Department of State, accessed March 8, 2018, www.state.gov/r/gec/.

439 Gardiner Harris, "State Dept. Was Granted 120 Million to Fight Russian Meddling. It Has Spent 0," *New York Times*, March 4, 2018, https://www.nytimes.com/2018/03/04/world/europe/state-department-russia-global-engagement-center.html.

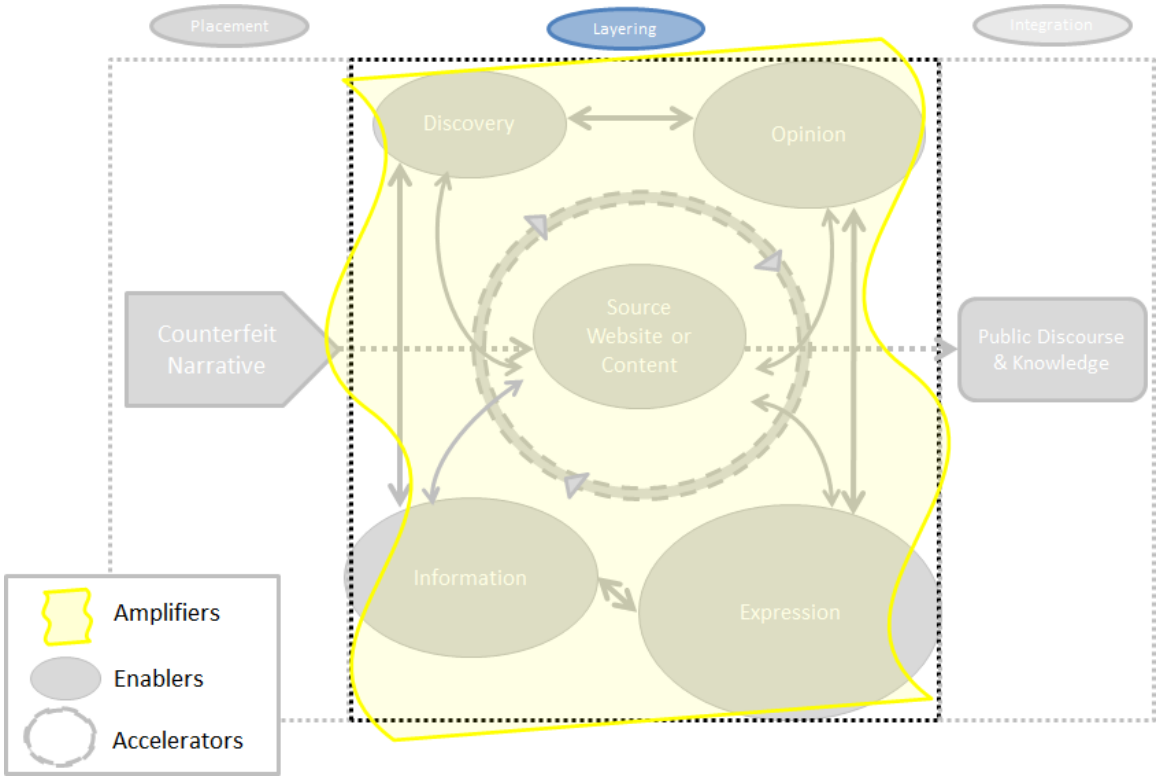

Figure 7. Attacking the Amplifiers

In February 2018 the Senate Intelligence Committee held a hearing concerning U.S. adversaries' use of cyber capabilities to achieve "strategic and malign objectives."[440] During the hearing, testimonies from the directors of the National Security Agency (NSA), the Office of the Director of National Intelligence, the Central Intelligence Agency (CIA), the Defense Intelligence Agency, the FBI, and the National Geospatial-Intelligence Agency impressed that these countries will continue to employ malicious cyber tactics unless they face severe repercussions. Director of National Intelligence Coats testified that "some of these actors, including Russia, are likely to pursue even more aggressive cyber attacks with the intent of degrading our democratic values and weakening our alliances."[441] Further, CIA Director Mike Pompeo, Director of National Intelligence

[440] "Global Threats and National Security," C-SPAN video, February 13, 2018, https://www.c-span.org/video/?440888-1/fbi-director-rob-porter-background-check-completed-july.

[441] C-SPAN, 20:27.

Coats, and NSA Director Admiral Michael Rogers each testified that the Intelligence Community is aware of Russian intentions to impact the 2018 election cycle[442]

Two weeks later, during a Department of Defense budget hearing, Admiral Rogers—who in addition to directing the NSA is also commander of U.S. Cyber Command—testified about the dramatic evolution of the cyberspace domain. The United States continues to face national and economic cyber threats, he explained, that have increased in "sophistication, magnitude, intensity, volume, and velocity."[443] He further testified: "Our adversaries have grown more emboldened, conducting increasingly aggressive activities to extend their influence without fear of significant consequence. We must change our approaches and responses here if we are going to change this dynamic."[444] Admiral Rogers believes that if the United States does not maintain superiority in the cyber domain, all our other domains will be threatened. During his testimony, he was asked if the United States was doing enough to combat the Russian influence operations, especially those targeted at our elections. He said that our current strategies, whether cyber, diplomatic, economic, or otherwise, have not deterred the Russians, nor have they altered the Russians' tactics.[445] He explained, however, that the Department of Defense does not have the legal authority to intervene throughout this problems space—even to defend the election systems.[446] What is or is not authorized, or what should or should not be authorized, is outside the scope of this thesis, but should certainly be considered by future researchers.

With this in mind, we should consider leveraging homeland security partners, especially state and local intelligence fusion centers, which are not subject to the same intelligence oversight as the federal government. Under their different rules and different mission, they may be able to help identify and disrupt disinformation campaigns.

---

[442] C-SPAN, 1:28:30.

[443] "Fiscal Year 2019 Cyber Command Budget Request," C-SPAN video, February 27, 2018, 10:21, https://www.c-span.org/video/?441677-1/nsa-chief-testifies-fiscal-year-2019-budget.

[444] C-SPAN, 10:54.

[445] C-SPAN, 58:36; 1:41:20.

[446] C-SPAN, "Global Threats and National Security," 1:17:35.

E. INOCULATE AGAINST INTEGRATION

Regardless of productive steps toward prevention and deterrence, information laundering will probably never be eliminated. It is difficult to identify when information truly becomes a counterfeit narrative, and emerging technologies that accelerate the problem are being adopted every day. Information laundering, by its very nature, is designed to sow chaos and discord. However, we might consider a valuable lesson from Sun Tzu's renowned *Art of War*: "Chaos drains energy, but drains less from the side already prepared for the chaotic environment."[447] Therefore, we must take steps to educate the public about this issue in order to prepare them for the chaotic environment. The chart in Figure 8 shows where this strategy falls on the Information Laundering 2.0 model.

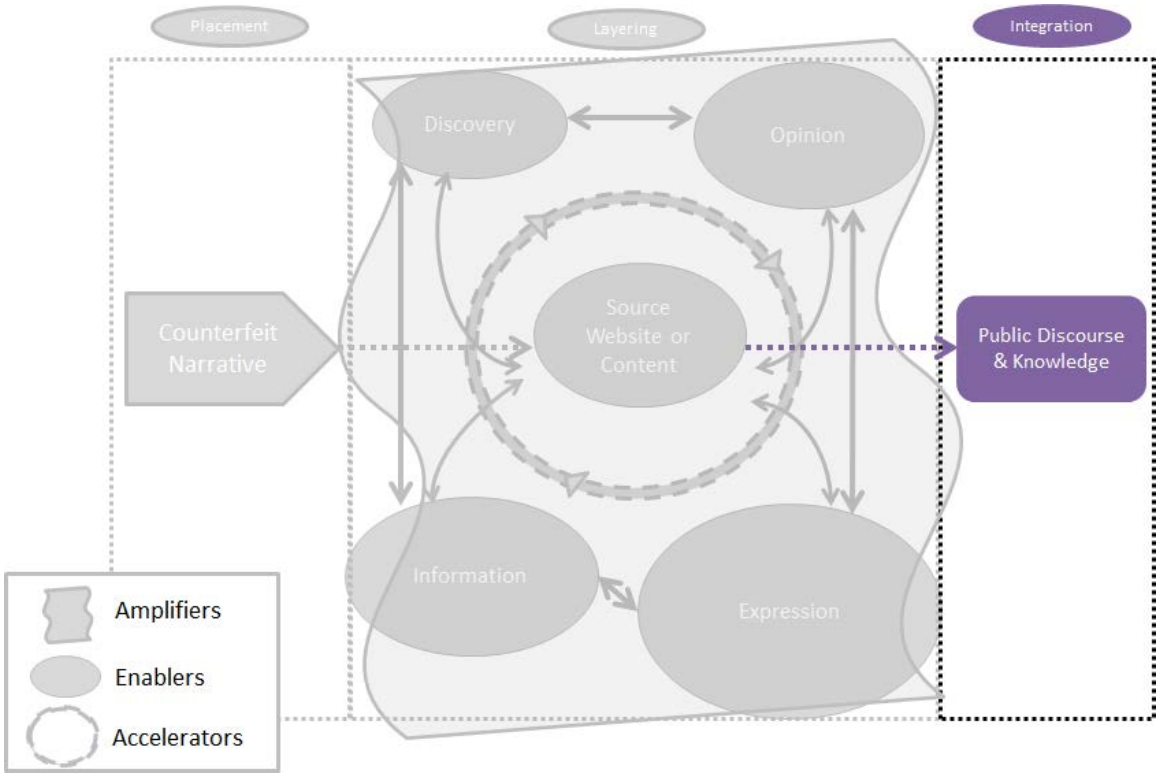

Figure 8. Inoculating against Integration

[447] Herrmann, "Nine Links in the Chain."

Bruce Wharton, acting under secretary for public diplomacy and public affairs at Stanford University, argues, "The way to counter pseudo-facts and misinformation is to present a compelling narrative of our own."[448] In the *Debunking Handbook*, John Cook with the Global Change Institute at the University of Queensland and Stephan Lewandowsky with the University of Western Australia similarly assert that "to successfully impart knowledge, communicators need to understand how people process information, how they modify their existing knowledge and how worldviews affect their ability to think rationally."[449] They go on to offer two useful tools for overcoming the backfire effect. First, we must reach out to the undecided majority, rather than the minority of individuals whose views are already strongly held. And second, we must develop messages that reduce the psychological effects that create resistance, including self-affirmation techniques and framing. From a cognitive standpoint, the mind prefers an "incorrect model over an incomplete model."[450] Therefore, when providing evidence to debunk misinformation, providing the true alternative explanation for the events is critical. For example, it is much easier to prove that a falsely accused suspect is not, in fact, a murderer if there is strong evidence pointing to the *actual* murderer; supplying evidence to incriminate the true guilty party is more effective than trying to prove that the innocent person did not commit the crime.[451] Of course, the alternative explanation offered must be plausible, and must cover all aspects of the event or concept.[452] Further, the use of graphics to clearly articulate an argument has been proven to increase the argument's effectiveness.[453] Many information launders use this tactic to increase the effectiveness of their counterfeit narratives. It would behoove us to understand this capability and leverage it to enhance the effectiveness of factual information.

---

[448] Wharton, "Public Diplomacy," 8–9.

[449] Cook and Lewandowsky, *Debunking Handbook*, 1.

[450] Cook and Lewandowsky, 5.

[451] Cook and Lewandowsky, 5.

[452] Cook and Lewandowsky, 5.

[453] Cook and Lewandowsky, 5.

During emergencies and natural disasters, when the effects of information laundering are often the most life-threatening, the SMWGESDM recommends utilizing "virtual operation support teams" or other partners to review social media and identify misinformation.[454] This information can be reported to officials, who can make efforts to correct it, and should also be synthesized on a central website where all rumors can be fact checked by the general public.[455] The SMWGESDM also recommends identifying the online influencers in a given community and asking them to disseminate critical and factual information during a time of crisis. Further, they recommend training and exercises for first responders and other volunteers that will help them identify misinformation online.[456]

F. MAKE INFORMATION LAUNDERING A CRIME AND FACTUAL INFORMATION A RIGHT

First and foremost, the United States needs to recognize the threat posed by information laundering, and needs to enact cyber mission strategies to combat it. When it comes to cyber defense capabilities, the Department of Defense is currently the leading federal defense agency, with the FBI as the leading law enforcement agency and the Department of Homeland Security in charge of critical infrastructure. In his policy recommendations, Chessen suggests that Congress designate the Department of Homeland Security, through its Office of Cybersecurity and Communications, as the lead agency to combat the spread of disinformation.[457] However, when considering information laundering from a criminal perspective, the mission may also be relevant for the FBI. Regardless of which federal entities ultimately acquire the responsibility, true cyber threat identification, sharing, and mitigation needs to be achieved across all agencies, including state and local governments and the private sector. The chart in Figure 9 shows where this strategy falls on the Information Laundering 2.0 model.

---

[454] SMWGESDM, "Countering Misinformation."

[455] SMWGESDM.

[456] SMWGESDM.

[457] Chessen, "The MADCOM Future," 17.

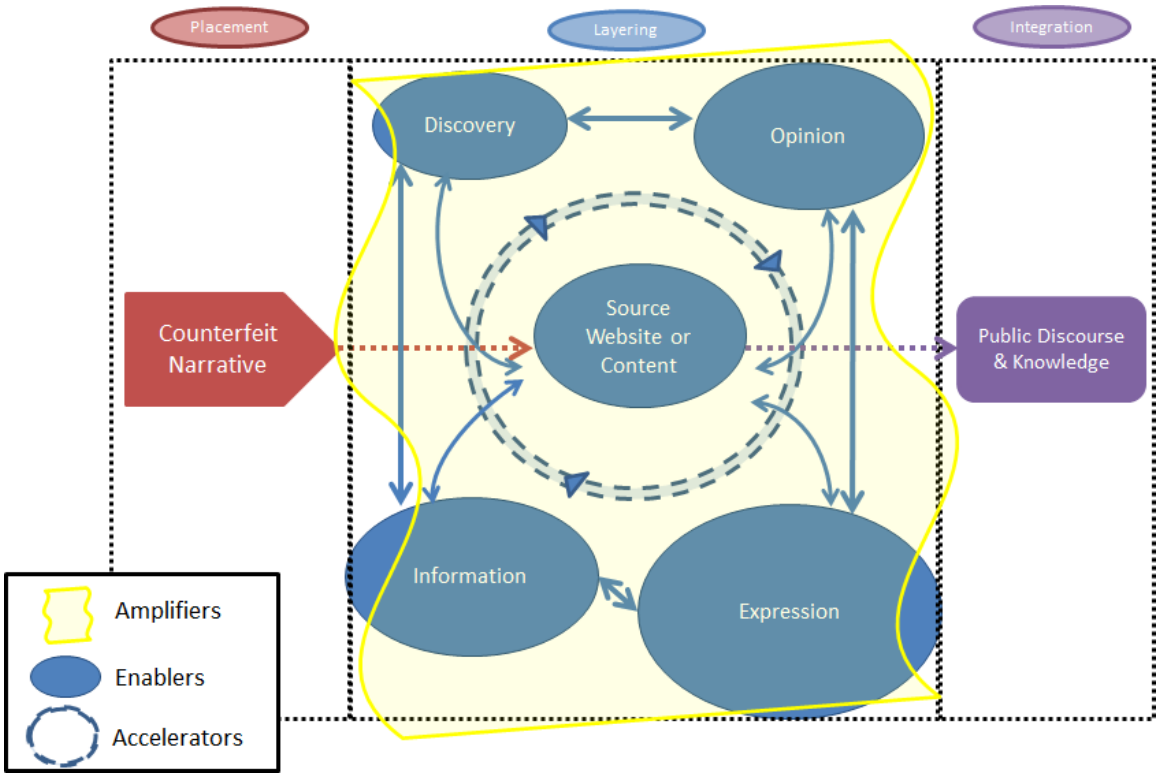

Figure 9. Criminalizing Information Laundering

As a result, we should explore ways to leverage the capabilities and unique access of state and local partners. The overall purpose of a fusion center is to gather information from local law enforcement, homeland security, public safety, and private-sector entities and fuse it with intelligence collected and produced by the federal Intelligence Community to better understand our "environments as they relate to the risk and threat of crime, terrorism, and other crises."[458] Seventy-nine fusion centers make up the National Network of Fusion Centers, and each one is uniquely positioned to operate in its area of responsibility while maintaining cohesion with the national homeland security strategy. The fusion centers have unique partnerships with local, county, state, tribal, and territorial partners, as well as with the private sector. These relationships can be crucial when trying to identify and combat disinformation associated with events, incidents, or issues within

[458] Justin Lewis Abold, Ray Guidetti, and Douglas Keyer, "Strengthening the Value of the National Network of Fusion Centers by Leveraging Specialization: Defining Centers of Analytical Excellence," *Homeland Security Affairs* 8, no. 7 (June 2012), https://www.hsaj.org/articles/223; John Rollins, *Fusion Centers: Issues and Options for Congress* (Washington, DC: Congressional Research Service, 2008), 5–6.

fusion centers' areas of responsibility. Further, the National Network of Fusion Centers is continuing to build its capabilities within the cyber threat intelligence realm and should consider incorporating combating information laundering into its cyber mission-set.

From a global perspective, developing regulation to combat the use of information warfare against nations would be a step in the right direction—especially if we want to counter ideological and financial amplifiers such as Russia and Macedonia. We must also start a conversation about what is acceptable not just in a nation-against-nation capacity, but also *within* a nation. For example, an authoritarian government looking to control the domestic narrative often finds that online content manipulation is much easier and more difficult to detect than blocking websites or arresting individuals for internet activity.[459] While information laundering occurring in other countries with no direct link to the United States may seem trivial, we must remember that the internet blurs the line between boundaries, nations, and jurisdictions. What impacts the understanding of truth, trust in government, and international sentiment in one country can have huge implications within the global online ecosystem.

On February 16, 2018, during opening remarks at the Munich Security Conference, United Nations Secretary-General Antonio Guterres called for a discussion on global rules related to cybersecurity.[460] He discussed the lack of an international consensus on how to regulate the so-called "Internet of things," and offered:

> I am one of those that defend that only through a multiple stakeholder approach we will be able to make progress. I believe it is necessary to bring together Governments, the private sector involved in these areas, civil society, academia and research centres, in order to be able to establish at least some basic protocols to allow for the web to be an effective instrument for the good.[461]

---

[459] Freedom house, "Manipulating Social Media," 2.

[460] "From Nuclear Threat to Cyberwar, Unity Must Prevail over Division in Tackling Global Challenges, Secretary-General Tells Security Forum," United Nations, February 16, 2018, www.un.org/press/en/2018/sgsm18900.doc.htm.

[461] United Nations.

Guterres believes we must have this conversation now, especially considering artificial intelligence's potential existential threat to humanity.[462] Clearly, more traditional cybersecurity threats, such as taking websites offline, stealing private data, hacking into opponents' machines for surveillance efforts, and conducting Distributed Denial of Service (DDoS) attacks, just to name a few, would be incorporated into the conversation.[463] However, these traditional attacks often overlap with those used for information laundering and therefore could be addressed as well. For example, as a means of spreading disinformation, hackers will hijack the accounts of opponents and use those accounts to spread their messaging.[464]

G. GET EDUCATED AND DEMAND MORE

Government officials, homeland security practitioners, and individuals throughout the country need to be more aware of and more informed about both cybersecurity and widespread online disinformation. While it is not essential for every single person to understand the nooks and crannies of the ecosystem, all people do need to understand that disinformation campaigns exist. In the physical world, they should demand more of themselves and their communities as it relates to critical thinking, fact checking, and becoming informed citizens. Our education system needs to be reviewed, revised, and retooled to emphasize not only literacy, numeracy, and critical thinking, but also sophisticated consumption of information. In the world of iPads, Alexas, and big data, traditional lessons—like teaching cursive—seem archaic; media literacy and consumption seem all the more pressing.

As mentioned, information laundering should be combatted at all stages of the process. However, first and foremost, policymakers, government officials, law enforcement, and homeland security professionals must have a better understanding of the tactics, techniques, and procedures used throughout the process. Also, they must keep themselves appraised of the threat from emerging technologies, and be prepared to have a

---

[462] United Nations.

[463] Freedom House, "Manipulating Social Media," 18–19.

[464] Freedom House, 11.

debate over these technologies as needed. Mark Goodman explains that "the goal is for citizens to have a basic understanding of how the technologies around them operate, not just so that they can use these tools to their full advantage, but also so that others cannot take advantage of their technological ignorance and harm them."[465] Further, new national strategies and incentives to educate the population about technology and cybersecurity, and to recruit them for the public sector, must be employed. Senator David Perdue, in his Department of Defense Cyber Command testimony, indicated that "we're going to be about 1.8 million cyber warriors short over the next five years."[466] We must develop incentives for training and education in information security and technology, and create better opportunities for these trained individuals to work for the government. Additionally, while emerging technologies such as artificial intelligence may pose challenges to cognitive security, when coupled with a coherent strategy, they may also offer solutions for countering information laundering.

Understanding counterfeit narratives and information laundering may merely be the first step in a very long and complex journey. But it provides us an essential framework to begin this important conversation. If people understand that this process is malicious, and detrimental to the health of an ecosystem, they will understand the importance of protecting the collective intelligence that can develop from the decentralized, heterogeneous space offered by the internet. Chessen suggests that "collective intelligence systems, in which large numbers of verified humans curate and validate the accuracy of information, are a possible solution to the overall disinformation problem."[467] Couple those verified humans with innovative artificial intelligence solutions, while using the information laundering model as a guide, and we can take actionable steps to protect the nation. Finally, the government should sponsor research and analysis related to a number of factors, including the influence of information laundering on persuasion, cognitive psychology, and mobilization to action, as well as on the information laundering process as a whole. In light of recent research about the spreadability of false information on social media, we also

---

[465] Goodman, *Future Crime*, 457.

[466] C-SPAN, "Fiscal Year 2019 Cyber Command Budget Request," 41:15.

[467] Chessen, "The MADCOM Future," 21.

need to better understand how novelty, attention, and outrage play into both the virality and credibility of information shared online. We need to view freedom in a new frame—one in which individuals have the right to accurate and true information.

The United States must immediately recognize and seek to understand counterfeit narratives and information laundering, as well as the threats they pose to democracy and freedom. Policymakers should tackle these issues with laws that are not too broad to limit free speech or freedom of the press, but that are effective enough to provide citizens with their right to be "secure in their persons" by establishing and defending cognitive security. Meanwhile, law enforcement and homeland security officials should make efforts to prepare for, and help mitigate, the confusion and tension that ultimately arise from these narratives, and prepare to protect themselves and the general public from incidents that, without intervention, could escalate to violence.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abold, Justin Lewis, Ray Guidetti, and Douglas Keyer. "Strengthening the Value of the National Network of Fusion Centers by Leveraging Specialization: Defining Centers of Analytical Excellence." *Homeland Security Affairs* 8, no. 7 (June 2012). https://www.hsaj.org/articles/223.

Allenby, Brad, and Joel Garreau. "Weaponized Narrative: The New Battlespace." White paper, The Center on the Future of War, 2017. http://azhumanities.org/wp-content/uploads/2017/08/WN-weaponized-narrative_final_compressed.pdf.

Aristotle. *On Rhetoric: A Theory of Civic Discourse, 2nd Edition*, translated by George A. Kennedy, 2nd edition. Oxford: Oxford University Press, 2006. www.amazon.com/Rhetoric-Theory-Civic-Discourse-2nd/dp/0195305094/ref=dp_ob_title_bk.

Barkun, Michael. *A Culture of Conspiracy: Apocalyptic Visions in Contemporary America (Comparative Studies in Religion and Society)*, 2nd edition. Berkeley: University of California Press, 2013. www.amazon.com/dp/B00DNJD46C/ref=docs-os-doi_0.

Berger, J.M., and Jonathon Morgan. "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter." Analysis paper no. 20, Brookings, 2015. www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

Bernays, Edward. *Propaganda*, Kindle edition. New York: Ig Publishing, 2004.

Bessi, Alessandro, Fabiana Zollo, Michela Del Vicario, Michelangelo Puliga, Antonio Scala, Guido Caldarelli, Brian Uzzi, and Walter Quattrociocchi. "Users Polarization on Facebook and YouTube." *PloS One* 11, no. 8 (August 2016): 1–24.

Borrowman, Shane. "Critical Surfing: Holocaust Denial and Credibility on the Web." *College Teaching* 47, no. 2 (Spring 1999): 44–47.

Brown, Heather, Emily Guskin, and Amy Mitchell. "The Role of Social Media in the Arab Uprisings." Pew Research Center, November 28, 2012. www.journalism.org/2012/11/28/role-social-media-arab-uprisings/.

Brown, Pete. "More than Half of Facebook Instant Articles Partners May Have Abandoned it." *Columbia Journalism Review*, February 2, 2018. https://www.cjr.org/tow_center/are-facebook-instant-articles-worth-it.php.

Carey, Alex. *Taking the Risk Out of Democracy: Corporate Propaganda versus Freedom and Liberty (History of Communication)*, 1st edition. Champaign: University of Illinois Press, 1996. https://www.amazon.com/Taking-Risk-Out-Democracy-Communication/dp/0252066162/ref=sr_1_1?s=books&ie=UTF8&qid=1512963129&sr=1-1&keywords=taking+the+risk+out+of+democracy.

Chessen, Matt. *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, And Threaten Democracy ... And What Can Be Done about it*. Washington, DC: Atlantic Council, 2017. http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.

———. "Understanding the Psychology Behind Computational Propaganda." In *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, edited by Shaun Powers and Markos Kounalakis, 19–24. Washington, DC: United States Advisory Commission on Public Diplomacy, 2017.

Chivvis, Christopher S. *Understanding Russian 'Hybrid Warfare' and What Can Be Done about it*. Santa Monica, CA: RAND, 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Conover, Adam. "Episode 44: Dr. Daniel Jolley on Why Conspiracy Theories Are Harmful." *Adam Ruins Everything* (podcast), January 24, 2018. www.maximumfun.org/adam-ruins-everything/adam-ruins-everything-episode-44-professor-daniel-jolley-why-conspiracy-theori.

Conway, Maura. "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research." *Studies in Conflict and Terrorism* 40, no. 1 (January 2, 2017): Foreword.

Cook, John, and Stephan Lewandowsky. *The Debunking Handbook*. St. Lucia, Australia: University of Queensland, 2013. http://sks.to/debunk.

Countering Violent Extremism Task Force. "Reference Aid: ISIS and Al-Qa'ida-Inspired Homegrown Violent Extremists." Department of Homeland Security, September 2017. www.dhs.gov/sites/default/files/publications/ISIS%20and%20AQ-Inspired%20Violent%20Extremists_CVE%20Task%20Force_Final.pdf.

Digital Shadows. "The Business of Disinformation: A Taxonomy Fake News Is More than a Political Battlecry." Accessed March 26, 2018. info.digitalshadows.com/rs/457-XEY-671/images/DigitalShadows-TheBusinessofDisinformationFakeNews.pdf

Divine, Doug, Toni Ferro, and Mark Zachry. "Work through the Web: A Typology of Web 2.0 Services." In *Proceedings of the 29th ACM International Conference on Design of Communication* (2011): 121–28.

Echeverría, Juan, and Shi Zhou. “The ‘Star Wars’ Botnet with >350k Twitter Bots.” Cornell University Library, June 13, 2017. 1, https://arxiv.org/abs/1701.02405.

Ellul, Jacques. *Propaganda: The Formation of Men’s Attitudes*, trans. Konrad Kellen and Jean Lerner. New York: Vintage, 1973. https://www.amazon.com/Propaganda-Formation-Attitudes-Jacques-Ellul/dp/0394718747/ref=sr_1_3?ie=UTF8&qid=1512952599&sr=8-3&keywords=jacques+ellul.

Farwell, James P. “The Media Strategy of ISIS.” *Survival* 56, no. 6 (November 2014): 49–55.

Federal Bureau of Investigation (FBI). “Combating the Growing Money Laundering Threat.” October 24, 2016. https://www.fbi.gov/news/stories/combating-the-growing-money-laundering-threat.

Flaxman, Seth, Sharad Goel, and Justin M. Rao. “Filter Bubbles, Echo Chambers, and Online News Consumption.” *Public Opinion Quarterly* 80, Special Issue (2016): 298–320.

Freedom House. “Manipulating Social Media to Undermine Democracy: Freedom on the Net 2017.” November 2017. https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf.

Gehl, Robert W. “The Case for Alternative Social Media.” *Social Media+ Society* 1, no. 2 (July–December, 2015): 1–12.

Goodman, Marc. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, Reprint edition. New York: Anchor, 2016. www.amazon.com/Future-Crimes-Digital-Underground-Connected/dp/0804171459/ref=sr_1_1?ie=UTF8&qid=1517711962&sr=8-1&keywords=future+crimes

Gossart, Cedric. “Can Digital Technologies Threaten Democracy by Creating-Information Cocoons.” In *Transforming Politics and Policy in the Digital Age*, edited by Jonathan Bishop, 145–154. Hershey, PA: IGI Global, 2014.

Gottfried, Jeffrey, and Elisa Shearer. “News Use across Social Media Platforms 2016.” Pew Research Center, May 26, 2016. http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/

Harris, Tristan. “How a Handful of Tech Companies Control Billions of Minds Every Day.” TED video, April 2017. https://www.ted.com/talks/tristan_harris_the_manipulative_tricks_tech_companies_use_to_capture_your_attention.

Hawley, George. *Right-Wing Critics of American Conservatism*. Lawrence: University Press of Kansas, 2016.

Herman, Edward S., and Noam Chomsky. *Manufacturing Consent: The Political Economy of the Mass Media*, Kindle edition. New York: Pantheon, 2011. https://www.amazon.com/Manufacturing-Consent-Political-Economy-Media-ebook/dp/B0055PJ4R0/ref=sr_1_1?ie=UTF8&qid=1514414505&sr=8-1&keywords=manufacturing+consent+noam+chomsky.

Herrmann, Jon. "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War." *The Strategy Bridge*, July 27, 2017. thestrategybridge.org/the-bridge/2017/7/27/nine-links-in-the-chain-the-weaponized-narrative-sun-tzu-and-the-essence-of-war.

Hitlin, Paul, Kenneth Olmstead, and Skye Toor. *Public Comments to the Federal Communications Commission about Net Neutrality Contain Many Inaccuracies and Duplicates*. Washington, DC: Pew Research Center, 2017. http://assets.pew research.org/wp-content/uploads/sites/14/2017/11/30155447/PI_2017.11.29_Net-Neutrality-Comments_FINAL.pdf.

Holcomb, Jesse, Jeffrey Gottfried, and Amy Mitchell. "News Use across Social Media Platforms." Pew Research Center, November 14, 2013. http://www.journal ism.org/2013/11/14/news-use-across-social-media-platforms/

Jasper, Scott, and Scott Moreland. "ISIS: An Adaptive Hybrid Threat in Transition." *Small Wars Journal*, October 29, 2016. https://calhoun.nps.edu/bitstream/handle/10945/50642/Jasper_Moreland_ISIS_%20An_Adaptive_Hybrid%20Threat_2016-10-29.pdf?sequence=1.

Jenkins, Henry, Sam Ford, and Joshua Green. *Spreadable Media: Creating Value and Meaning in a Networked Culture (Postmillennial Pop)*, Kindle edition. New York: NYU Press, 2013. https://www.amazon.com/Spreadable-Media-Creating-Networked-Postmillennial-ebook/dp/B00B1Q88EW/ref=tmm_kin_swatch_0?_encoding=UTF8&qid=1517784651&sr=8-1.

Jolley, Daniel, and Karen M. Douglas. "The Effects of Anti-vaccine Conspiracy Theories on Vaccination Intentions." *PloS One* 9, no. 2 (February 2014): e89177. https://doi.org/10.1371/journal.pone.0089177.

———. "The Social Consequences of Conspiracism: Exposure to Conspiracy Theories Decreases Intentions to Engage in Politics and to Reduce One's Carbon Footprint." *British Journal of Psychology* 105, no. 1 (February 2014): 35–56. https://doi.org/10.1111/bjop.12018.

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

Klein, Adam. "Slipping Racism into the Mainstream: A Theory of Information Laundering." *Communication Theory* 22, no. 4 (November 2012): 427–448.

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. “Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks.” *Proceedings of the National Academy of Sciences of the United States of America* 111, no. 24 (June 2014): 8788–8790. https://doi.org/10.1073/pnas.1320040111.

Le Bon, Gustave. *The Crowd: A Study of the Popular Mind*, Kindle edition. Overland Park, KS: Digireads, 2004. https://www.amazon.com/Crowd-Study-Popular-Mind-ebook/dp/B000FC230S/ref=pd_sim_351_7?_encoding=UTF8&psc=1&refRID=Z96WDJYACZVPEA5D667Y.

McCulloh, Timothy B., and Richard B. Johnson. *Hybrid Warfare*. JSOU Report 13-. (MacDill AFB, FL: JSOU, 2013.

Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook. “Misinformation and Its Correction: Continued Influence and Successful Debiasing.” *Psychological Science in the Public Interest* 13, no. 3 (December 2012): 106–131. https://doi.org/10.1177/1529100612451018.

Lundén, Kimmo. “The Death of Print? The Challenges and Opportunities Facing the Print Media on the Web.” Fellowship paper, University of Oxford, 2008. http://reutersinstitute.politics.ox.ac.uk/sites/default/files/The%20Death%20of%20Print%20-%20The%20Challenges%20and%20Opportunities%20facing%20the%20Print%20Media%20on%20the%20Web.pdf.

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. http://journals.sagepub.com/doi/abs/10.1177/0002764217701217.

Naughton, John, “The Evolution of the Internet: From Military Experiment to General Purpose Technology.” *Journal of Cyber Policy* 1, no. 1 (January 2016): 5–28. https://doi.org/10.1080/23738871.2016.1157619.

Neff, Gina, and Peter Nagy. “Automation, Algorithms, and Politics | Talking to Bots: Symbiotic Agency and the Case of Tay.” *International Journal of Communication Systems* 10 (October 2016): 4915–4931. http://ijoc.org/index.php/ijoc/article/view/6277/1804.

Neo, Loo Seng, Leevia Dillon, Priscilla Shi, Jethro Tan, Yingmin Wang, Danielle Gomes, and Majeed Khader. “Understanding the Psychology of Persuasive Violent Extremist Online Platforms.” In *Combating Violent Extremism and Radicalization in the Digital Era*, 1–15. Hershey, PA: IGI Global, 2016.

Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, David A. L. Levy, and Rasmus Kleis Nielsen. *Reuters Institute Digital News Report 2017*. Oxford: Reuters Institute, 2017. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf?utm_source=digitalnewsreport.org&utm_medium=referral.

Nickerson, Raymond S. "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises." *Review of General Psychology* 2, no. 2 (1998): 175–220. http://psy2.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf.

Office of the Director of National Intelligence (ODNI). *Assessing Russian Activities and Intentions in Recent US Elections.* Washington, DC: ODNI, 2017.

Park, Jaehong, Prabhudev Konana, Bin Gu, Alok Kumar, and Rajagopal Raghunathan. "Information Valuation and Confirmation Bias in Virtual Communities: Evidence from Stock Message Boards." *Information Systems Research* 24, no. 4 (December 2013): 1050–1067.

Paul, Christopher, and Miriam Matthews. *The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter it*. Santa Monica, CA: RAND, 2016.

PEN America. F*aking News: Fraudulent News and the Fight for Truth*. New York: PEN America, 2017. https://pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf.

Pratkanis, Anthony, and Elliot Aronson. *Age of Propaganda: The Everyday Use and Abuse of Persuasion*. New York: Holt Paperbacks, 2001. www.amazon.com/Age-Propaganda-Everyday-Abuse-Persuasion/dp/0805074031/ref=sr_1_1?ie=UTF8&qid=1512962691&sr=8-1&keywords=pratkanis+and+aronson.

Rao, T. S. Sathyanarayana, and Chittaranjan Andrade. "The MMR Vaccine and Autism: Sensation, Refutation, Retraction, and Fraud." *Indian Journal of Psychiatry* 53, no. 2 (April 2011): 95–96. https://doi.org/10.4103/0019-5545.82529.

Rid, Thomas, and Marc Hecker. *War 2.0: Irregular Warfare in the Information Age.* Santa Barbara, CA: Praeger, 2009. https://www.amazon.com/War-2-0-Irregular-Information-International/dp/0313364702/ref=sr_1_2?ie=UTF8&qid=1510502399&sr=8-2&keywords=war+2.0.

Rollins, John. *Fusion Centers: Issues and Options for Congress*. Washington, DC: Congressional Research Service, 2008.

Schiffrin, Anya. "How Europe Fights Fake News." *Columbia Journalism Review*, October 26, 2017. https://www.cjr.org/watchdog/europe-fights-fake-news-facebook-twitter-google.php.

Sedensky, Stephen J. III. “Report of the State’s Attorney for the Judicial District of Danbury on the Shootings at Sandy Hook Elementary School.” Report, State of Connecticut Division of Criminal Justice, 2013. http://www.ct.gov/csao/lib/csao/Sandy_Hook_Final_Report.pdf.

Shao, Chengcheng, Givoanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, and Filippo Menzer. “The Spread of Fake News by Social Bots.” Cornell University Law Library, July 24, 2017. http://arxiv.org/abs/1707.07592.

Shearer, Elisa, and Jeffrey Gottfried. “News Use across Social Media Platforms 2017.” Pew Research Center, September 7, 2017. http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

Shultz, H.R., and R. Godson. *Dezinformatsia: Active Measures in Soviet strategy*. Washington, DC: Pergamon Brassey’s, 1984.

Smith, Naomi, and Tim Graham. “Mapping the Anti-vaccination Movement on Facebook.” *Information, Communication and Society* (December 2017): 1–18. https://doi.org/10.1080/1369118X.2017.1418406.

Social Media Working Group for Emergency Services and Disaster Management (SMWGESDM). “Countering Misinformation, Rumors, and False Information on Social Media before, during, and after Disasters and Emergencies.” Department of Homeland Security, March 2018. https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf

Starbird, Kate. “Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter.” Paper presented at the 11th International Conference on Web and Social Media, Montreal, Canada, May 15–18, 2017).

State of Connecticut Office of the Child Advocate. “Shooting at Sandy Hook Elementary School.” Rreport, State of Connecticut, 2014. http://www.ct.gov/oca/lib/oca/sandyhook11212014.pdf

State of Michigan. “Flint Water Advisory Task Force Final Report.” March 2016. http://www.michigan.gov/documents/snyder/FWATF_FINAL_REPORT_21March2016_517805_7.pdf.

Stempel, Carl, Thomas Hargrove, and Guido H. Stempel III. “Media Use, Social Structure, and Belief in 9/11 Conspiracy Theories.” *Journalism and Mass Communication Quarterly* 84, no. 2 (2007): 354–355.

Surowiecki, James. *The Wisdom of Crowds*, Reprint edition. New York: Anchor, 2005. https://www.amazon.com/dp/B000FCKC3I/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1.

Swire, Briony, Ullrich K. H. Ecker, and Stephan Lewandowsky. “The Role of Familiarity in Correcting Inaccurate Information.” *Journal of Experimental Psychology: Learning, Memory, and Cognition* 43, no. 12 (December 2017): 1948–1961. https://doi.org/10.1037/xlm0000422.

TED. “Sad in Silicon Valley.” *Sincerely, X* (podcast), August 10, 2017. https://art19.com/shows/sincerely-x/episodes/f7d7cf3f-9002-4ac2-b67c-6118fa44978e.

Tversky, Amos, and Daniel Kahneman. “Availability: A Heuristic for Judging Frequency and Probability.” *Cognitive Psychology* 5 (1973): 207–232. https://msu.edu/~ema/803/Ch11-JDM/2/TverskyKahneman73.pdf.

United Nations. “From Nuclear Threat to Cyberwar, Unity Must Prevail over Division in Tackling Global Challenges, Secretary-General Tells Security Forum.” February 16, 2018. https://www.un.org/press/en/2018/sgsm18900.doc.htm.

U.S. Department of Justice. “Participant Guide—Basic Financial Investigations Seminar.” Seminar, U.S. Department of Justice, 2013.

van Dijck, Jose. *The Culture of Connectivity: A Critical History of Social Media*, 1st edition. Oxford: Oxford University Press, 2013. www.amazon.com/Culture-Connectivity-Critical-History-Social-ebook/dp/B00AWOTA96/ref=mt_kindle?_encoding=UTF8&me=.

VICE News. “Facebook’s Reckoning & Free Money in Finland: VICE News Tonight Full Episode (HBO).” YouTube video, November 7, 2017. www.youtube.com/watch?v=ACiXq_lBWlY&list=PLw613M86o5o5h_7QkuryiioEJDG0eI07V&index=20.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. “The Spread of True and False News Online.” *Science* 359, no. 6380 (March 2018): 1146–1151. https://doi.org/10.1126/science.aap9559.

Weatherall, James Owen, Cailin O’Connor, and Justin Bruner. “How to Beat Science and Influence People: Policy Makers and Propaganda in Epistemic Networks.” Cornell University Library, January 4, 2018. http://arxiv.org/abs/1801.01239.

Wharton, Bruce. “Remarks on ‘Public Diplomacy in a Post-truth Society.’” In *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, edited by Shaun Powers and Markos Kounalakis, 7–11. Washington, DC: United States Advisory Commission on Public Diplomacy, 2017.

Wojcieszak, Magdalena, and Vincent Price. “What Underlies the False Consensus Effect? How Personal Opinion and Disagreement Affect Perception of Public Opinion.” *International Journal of Public Opinion Research* 21, no. 1 (March 2009): 25–46. https://doi.org/10.1093/ijpor/edp001.

Woolley, Samuel C. “Computational Propaganda and Political Bots: An Overview.” In *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*, edited by Shaun Powers and Markos Kounalakis. Washington, DC: United States Advisory Commission on Public Diplomacy, 2017.

Woolley, Samuel C., and Philip N. Howard. “Computational Propaganda Worldwide: Executive Summary.” Working paper, University of Oxford, 2017. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

World Economic Forum. “Digital Wildfires in a Hyperconnected World.” Accessed January 24, 2017. http://wef.ch/GJCg5E.

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