2019
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Combatting Targeted Disinformation Campaigns

A whole-of-society issue

October 2019

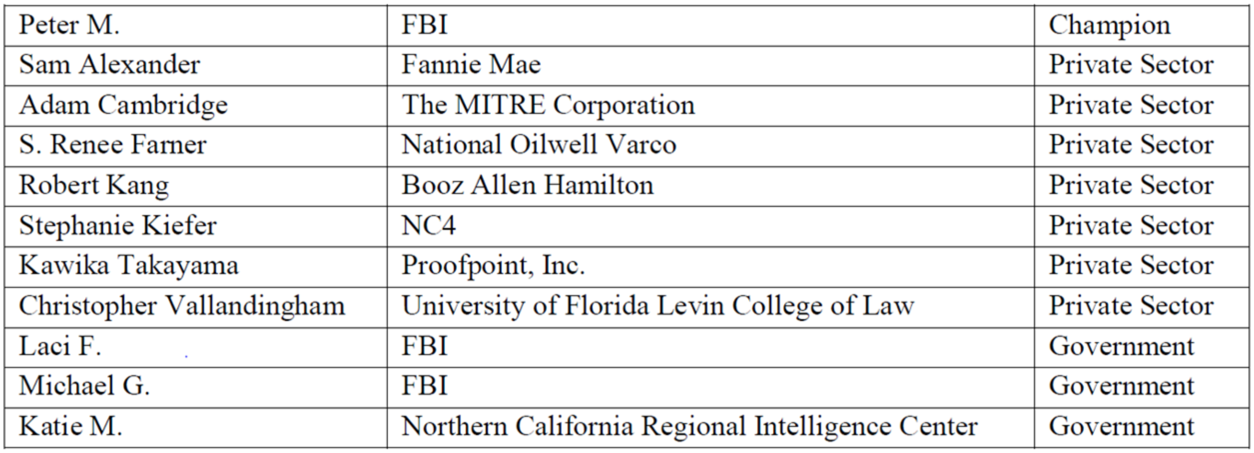
ACKNOWLEDGMENTS

We would first like to thank the Office of the Director of National Intelligence and the Department of Homeland Security for their thoughtful support throughout the duration of the program.

We are also very thankful for the unique insights we received from contacts and interviewees who contributed their time and information to this report by educating our group on the many aspects of how disinformation campaigns are conducted, the technologies involved, and the legal, regulatory, and policy landscape that affects how we confront this issue. The suggestions on further areas for exploration identified through our conversations have also helped considerably in the shaping of this paper, and where we would like our future research endeavors to go.

The people stepping up to help provide information for this project included private industry experts from technology and social media companies, university and think tank scholars and researchers, and state and federal agencies. We would like to acknowledge all the Team Members and Champion listed below for their contributions to this project and this report. This report would not have been possible without the diverse public and private sector makeup of this team and their legal, technical, academic, and policy expertise.

Team Members



Peter M.	FBI	Champion
Sam Alexander	Fannie Mae	Private Sector
Adam Cambridge	The MITRE Corporation	Private Sector
S. Renee Farner	National Oilwell Varco	Private Sector
Robert Kang	Booz Allen Hamilton	Private Sector
Stephanie Kiefer	NC4	Private Sector
Kawika Takayama	Proofpoint, Inc.	Private Sector
Christopher Vallandingham	University of Florida Levin College of Law	Private Sector
Laci F.	FBI	Government
Michael G.	FBI	Government
Katie M.	Northern California Regional Intelligence Center	Government

EXECUTIVE SUMMARY

In today's information environment, the way consumers view facts, define truth, and categorize various types of information does not adhere to traditional rules. The shift from print sources of information to online sources and the rise of social media have had a profound impact on how consumers access, process, and share information. These changes have made it easier for threat actors to spread disinformation and exploit the modern information environment, posing a significant threat to democratic societies. Accordingly, disinformation campaigns should be viewed as a whole-of-society problem requiring action by government stakeholders, commercial entities, media organizations, and other segments of civil society.

Outline

Before the 2016 U.S. presidential election, disinformation was not at the forefront of American discourse. U.S. government efforts in the disinformation arena had focused primarily on combatting transnational terrorist organizations. Social media companies were just becoming aware how their platforms empowered threat actors on a large scale. Mainstream media organizations were not yet plagued by accusations of spreading "fake news" and fears of concerted foreign efforts to undermine American society had not seeped into the consciousness of the general public.

Since the presidential election, disinformation campaigns have been the subject of numerous investigations, research projects, policy forums, congressional hearings and news reports. The end result has been a better understanding of the methods and motives of threat actors engaging in disinformation campaigns and the impact of these campaigns, which in turn has led to improved efforts to combat these campaigns and minimize the harm they cause.

Until the end of 2018, much of the work on disinformation campaigns was post-mortem—after the campaign had nearly run its course. At that point, the desired effect of the threat actor had been achieved and the damage done. Since late 2018, civil society groups, scholars, and investigative journalists have made great strides in identifying ongoing disinformation campaigns and sharing findings with social media platforms, who then remove inauthentic accounts. However, these campaigns are often identified after the disinformation has already entered and been amplified inside the information environment, too late to fully negate the harm.

The extent of private and public sector cooperation over the next five years to address targeted disinformation campaigns will determine the direction of the issue. We view this issue as a whole-of-society problem requiring a whole-of-society response. The purpose of this paper is to provide a framework for stakeholders to understand the lifecycle of disinformation campaigns, then to recommend a preliminary set of actions that may assist with the identification and neutralization of a disinformation campaign before disinformation is amplified within the information environment, thus mitigating its impact.

The framework recommends actions for a variety of stakeholders to combat targeted disinformation campaigns by neutralizing threat actors, bolstering social media technology to make it less susceptible to exploitation, and building public resilience in the face of disinformation.

We recommend:

- Support for government legislation promoting transparency and authenticity of online political content. We support passage of the Honest Ads Act, which would hold digital political advertising to the same disclosure requirements as those required for political advertisements on television, radio and print media.

- Funding and support of research efforts that bridge the commercial and academic sectors. Academic research efforts, armed with the appropriate real-world data from commercial platforms, could more effectively explore the trends and methodologies of targeted disinformation campaigns. This research could also help to better identify segments of the population most susceptible to disinformation campaigns and guide resources for media literacy efforts. This research should also include the development of technical tools to analyze disinformation across platforms and identify inauthentic content such as deep fakes.

- Establishment of an information sharing and analysis organization to bring together government entities, research institutions and private-sector platforms. The organization could facilitate information exchange through a trusted third-party. The organization could serve as an information center that would pool expertise and track disinformation trends and methods.

- Encouragement of media organizations to promote the need for healthy skepticism by their users when consuming online content. This includes providing media literacy resources to users and enhancing the transparency of content distributors.

- Expansion of media literacy programs to build societal resilience in the face of disinformation campaigns. Media literacy could be framed as a patriotic choice in defense of democracy. Public education through advocacy groups like AARP, which can tailor the message of media literacy for their members, could be an effective means of encouraging the adoption of healthy skepticism towards online information.

Scope

This paper was produced by the Combatting Targeted Disinformation Campaigns team, operating under the auspices of the Department of Homeland Security's Analyst Exchange Program. The paper was developed based on open source research and interviews with identified subject matter experts. All judgments and assessments are based soley on unclassified sources and are the product of joint public and U.S. government efforts and do not necessarily represent the judgments and assessments of the team members' employers.

DISINFORMATION OVERVIEW

Disinformation is not synonymous with false information or “fake news.” False information that is shared with others without the intent to mislead can be defined as misinformation. People share misinformation because they believe the information is true when, in fact, it is not.

On the other hand, the purpose of disinformation is to mislead. Disinformation is information created and distributed with the express purpose of causing harm.[1] Disinformation is not necessarily false information. Even true information can be presented in misleading ways and thus form the grist of a targeted disinformation campaign.

A targeted disinformation campaign, in the context of this paper, is more insidious than simply telling lies on the internet. One untrue meme or contrived story may be a single thread in a broader operation seeking to influence a target population through methods that violate democratic values, societal norms and, in some jurisdictions, the law.

A disinformation campaign occurs when a person, group of people, or entity (a “threat actor”) coordinate to distribute false or misleading information while concealing the true objectives of the campaign. The objectives of disinformation campaigns can be broad (e.g., sowing discord in a population) or targeted (e.g., propagating a counternarrative to domestic protests) and may employ all information types (disinformation, misinformation, malinformation, propaganda, and true information). The target of a disinformation campaign is the person or group the threat actor aims to influence in order to achieve the campaign’s objective.

Information Types

Propaganda has a political connotation and is often connected to information produced by governments (the lines between advertising, publicity, and propaganda are often unclear).

Disinformation is manufactured information that is deliberately created or disseminated with the intent to cause harm.

Misinformation is false information shared without the intent to mislead.

Malinformation is genuine information, typically private or revealing, that may be distributed in a campaign to cause harm to a person s reputation in furtherance of the campaign s objective.

Inauthentic Information is *not* transparent in its origins and affiliation. The source of the information tries to mask its origin and identity.

Authentic Information is transparent in its origins and affiliation. The source of the information is unhidden.

***Sources*:**

Claire Wardle, Information Disorder: The Essential Glossary, First Draft, Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2018, https://firstdraftnews.org/wp content/uploads/2018/07/infoDisorder_glossary.pdf?x 19860

Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East.” FireEye Intelligence, August 21, 2018, https://www.fireeye.com/blog/threat research/2018/08/suspected iranian influence operation.html

Targeted disinformation campaigns are not a new phenomenon and sophisticated ones follow a predictable progression. After establishing the objective, a threat actor follows distinct steps, discussed later in more detail: recon, build, seed, copy, amplify, and control to bring about an outcome. But first we will explore the history and impacts of these campaigns, the information environment that facilitates modern campaigns, and the motives of disinformation threat actors.

[1] Claire Wardle, “Information Disorder: The Essential Glossary,” First Draft. Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2018, https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x19860.

A Brief History of Influence Operations

To understand the role of disinformation in contemporary society, it is helpful to look at examples of how national governments, non-governmental organizations, and informal groups of individuals in modern history have used influence operations to sway public opinion both domestically and internationally. In international relations, the very essence of "soft power" is the ability to influence other nations through persuasion and other non-coercive means.

Within democratic societies, public support for policy and legislative initiatives is often critical for the success of these initiatives.[2] Eroding public support for U.S. involvement in the Vietnam War, not battlefield defeats, led to the eventual U.S. withdrawal from that conflict.[3] For decades, the U.S. Department of Agriculture promoted healthy eating habits through publication and distribution of nutrition guidelines.[4] In similar fashion, U.S. Surgeon General reports linking smoking and other tobacco use with cancer and other diseases, along with mandatory warning labels and limitations on advertisements for tobacco products, has helped lead to a precipitous decline in the U.S. smoking rate since the 1940s.

Nongovernmental organizations attempt to steer public opinion on a host of issues. Methods these organizations might use include editorials in newspapers, celebrity endorsements, chain e-mails, hosting public forums, publishing reports, organizing conferences, recording podcasts, and direct mail campaigns.

On the international front, within the U.S. Department of State, a core mission of the Bureau of Global Public Affairs is promotion of international support for the "values and policies of the United States."[5] Likewise, a core mission of the Peace Corps is "to help promote a better understanding of Americans on the part of the peoples served."[6]

Other countries, whether democratic or autocratic, also attempt to influence domestic and international audiences. Israeli Prime Minister Benjamin Netanyahu endeavored to undermine international support for the Iran nuclear deal.[7] China has attempted to polish its international reputation by spending vast sums of money worldwide to promote Chinese culture and allay the concerns of other countries uneasy about Chinese economic and military ambitions.[8] France has cultural centers in 137 countries to raise awareness of French culture.[9] And Russia has attempted to portray itself as a viable alternative to the West.[10]

Shaping public opinion through licit means is a legitimate function of government. However, there are many instances when governments have used illicit means to accomplish their objectives. During the First World War, false news stories about atrocities committed by the German Army served to demonize the

[2] Cheryl Boudreau and Scott A. Mackenzie, "Wanting What Is Fair: How Party Cues and Information about Income Inequality Affect Public Support for Taxes," *The Journal of Politics* 80, no. 2 (2018): 367–81, https://doi.org/10.1086/694784.

[3] W.L. Lunch and P. W. Sperlich, "American Public Opinion and the War in Vietnam," *Political Research Quarterly* 32, no. 1 (January 1979): 21–44, https://doi.org/10.1177/106591297903200104; William M. Darley, "War Policy, Public Support, and the Media," *The US Army War College Quarterly: Parameters*, 2005, 121–34, https://ssi.armywarcollege.edu/pubs/parameters/articles/05summer/darley.pdf.

[4] U.S. Department of Agriculture. "A Brief History of USDA Food Guides." Choose MyPlate, updated November 30, 2018, https://www.choosemyplate.gov/brief-history-usda-food-guides.

[5] U.S. Department of State, "Our Mission," Bureau of Global Public Affairs, accessed September 17, 2019, https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/bureau-of-global-public-affairs/.

[6] Peace Corps, "About Our Mission," accessed September 17, 2019, https://www.peacecorps.gov/about/.

[7] Katie Zezima. "Netanyahu Warns That Nuclear Deal 'Paves Iran's Path' to a Bomb." *Washington Post*, March 3, 2015, https://www.washingtonpost.com/news/post-politics/wp/2015/03/03/in-much-anticipated-speech-netanyahu-to-address-congress-tuesday/.

[8] "China Is Spending Billions to Make the World Love It," *The Economist*, March 23, 2017, https://www.economist.com/china/2017/03/23/china-is-spending-billions-to-make-the-world-love-it.

[9] Ministère de l'Europe et des Affaires étrangères, "France's Overseas Cultural Network," accessed September 17, 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/cultural-diplomacy/france-s-overseas-cultural-network/.

[10] Andrew Radin and Clint Reach, "Russian Views of the International Order," RAND Corporation, May 18, 2017, https://www.rand.org/pubs/research_reports/RR1826.html.

enemy in the eyes of the British public.[11] In the years leading up to the Second World War, a key objective of the Nazi propaganda machine was “to absorb the individual into a mass of like-minded people, and the purpose of the ‘suggestion’ was not to deceive but to articulate that which the crowd already believed.”[12] Soviet disinformation campaigns, so-called “active measures,” were central to the Soviet Union’s efforts to increase its influence throughout the world and undermine the influence of its rivals.[13] Soviet efforts to control the press of foreign countries, forge documents, and manipulate other countries’ societal infrastructure, including the academic, economic, and political spheres, were hallmarks of its organized disinformation efforts.[14] During the Cold War, the Soviet KGB and East German Stasi peddled the notion that the U.S. Department of Defense genetically engineered the human immunodeficiency virus (HIV).[15]

Impact of Disinformation Campaigns

The mere fact that domestic and foreign actors are engaging in disinformation campaigns against domestic audiences, especially during election cycles, is cause for concern irrespective of the success of these campaigns. Though it is often challenging to determine the full impact of disinformation campaigns, it is possible to identify, in some cases, short-term and long-term impacts. In the short term, targeted disinformation campaigns may:

- cause and exploit emotional reactions to sensational topics, causing disinformation to spread more rapidly than legitimate news.[16]
- aggravate existing societal fissures, inflaming ideological, political, gender-based, ethnic, and religious differences.[17] This heightened state of agitation may fuel acts of harassment and violence.[18]
- increase health risks. Disinformation campaigns aimed at health issues and the provision of health care may lead to sudden changes in dietary habits, the adoption of treatments which have not been scientifically verified, and engender distrust in the advice given by medical professionals.[19,20]

[11] Roy Greenslade, “First World War: How State and Press Kept Truth Off the Front Page,” *The Guardian*, July 27, 2014, https://www.theguardian.com/media/2014/jul/27/first-world-war-state-press-reporting.

[12] Nicholas O'Shaughnessy, “The Nazis' Propaganda Trick: Invite the Public to Help Create an Alternate Reality,” Slate, March 14, 2017, https://slate.com/news-and-politics/2017/03/how-nazi-propaganda-encouraged-the-masses-to-co-produce-a-false-reality.html.

[13] Fletcher Schoen and Christopher J. Lamb, “Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference (Strategic Perspectives, No. 11),” *Strategic Perspectives*, June 2012, https://doi.org/10.21236/ada577586.

[14] U.S. Department of State, “Soviet ‘Active Measures’ Forgery, Disinformation, Political Operations (Special Reports No. 88)”, October 1981, accessed September 17, 2019, https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

[15] Douglas Selvage and Christopher Nehring, “Operation ‘Denver’: KGB and Stasi Disinformation Regarding AIDS,” Wilson Center, July 22, 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids.

[16] Katie Langin, “Fake News Spreads Faster than True News on Twitter—Thanks to People, Not Bots,” *Science*, March 8, 2018, https://doi.org/10.1126/science.aat5350.

[17] Lisa Reppell and Erica Shein, “Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions,” International Foundation for Electoral Systems, April 2019, https://www.ifes.org/sites/default/files/2019_ifes_disinformation_campaigns_and_hate_speech_briefing_paper.pdf.

[18] Paul Mozur, “A Genocide Incited on Facebook, With Posts From Myanmar's Military,” *New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[19] Marc Trotochaud and Matthew Watson, “Misinformation and Disinformation: An Increasingly Apparent Threat to Global Health Security,” The Bifurcated Needle, Center for Health Security, John Hopkins University, November 29, 2018, http://www.bifurcatedneedle.com/new-blog/2018/11/29/misinformation-and-disinformation-an-increasingly-apparent-threat-to-global-health-security.

[20] Emma Woollacott, “The Viral Spread Of Ebola Rumors,” *Forbes*, October 9, 2014, https://www.forbes.com/sites/emmawoollacott/2014/10/09/the-viral-spread-of-ebola-rumors/#191c27f219d8.

- harm the reputations of individuals, governments, companies, and other organizations, even if the disinformation is later proven false. [21]
- cause panic that reverberates through financial markets and leads individuals to make unsound financial decisions. [22]

The long-term effects of disinformation campaigns are potentially serious to democratic societies. While there is no sure-fire method to predict the outcomes of disinformation campaigns, based on the analysis of available literature and discussions with experts in the public and private sectors, there are a number of possible outcomes. In the long term, disinformation campaigns may:

- manipulate and further radicalize domestic audiences through impersonating and amplifying their existing messaging.[23]
- blur the lines between authentic and inauthentic content.[24] By mimicking legitimate sources of information, actors engaging in disinformation campaigns make it more difficult for individuals to distinguish truth from fiction.
- increase distrust of all online information sources.[25] Disinformation campaigns make individuals less apt to view online news sources as credible and fact-based, potentially harming democratic outcomes since exposure to a variety of reliable information sources helps to fuel rational, informed decision-making. Absent reliable sources of information, individuals are more likely to succumb to decision-making based on emotional appeal and personal whim.[26]
- undermine trust in democracy and confidence in the ability of government institutions to solve societal problems.[27]

INFORMATION ENVIRONMENT

The Social Media Revolution

As the invention of the movable type machine in the 15th century revolutionized the way the public received and shared information, so did the invention and widespread use of social media platforms in the 21st century. Social media platforms have granted individuals the ability to create communities with other individuals who have shared views and ideologies far more easily than was possible before the emergence of these platforms.

[21] Amanda Seitz, “NOT REAL NEWS: Anderson Cooper Didn't Fake Flood Broadcast,” AP NEWS, September 18, 2018, https://www.apnews.com/f1b624dc8154458d8c193d3d6be341de; “2019 Brand Disinformation Impact Study,” New Knowledge, January 2019, https://www.newknowledge.com/articles/2019-brand-disinformation-impact-study/.

[22] Max Fisher, “Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?,” *Washington Post*, April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

[23] Alina Polyakova and Daniel Fried, “Democratic Defense Against Disinformation 2.0,” Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.

[24] Alina Polyakova and Daniel Fried, “Democratic Defense Against Disinformation 2.0,” Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.

[25] Katherine Costello, “Russia’s Use of Media and Information Operations in Turkey: Implications for the United States,” RAND Corporation, August 28, 2018, https://www.rand.org/pubs/perspectives/PE278.html; Paul Butcher, “Disinformation and Democracy: The Home Front in the Information War,” European Policy Centre, January 30, 2019, https://www.epc.eu/documents/uploads/pub_8984_disinformation.pdf?doc_id=2102.

[26] Paul Butcher, “Disinformation and Democracy: The Home Front in the Information War,” European Policy Centre, January 30, 2019, https://www.epc.eu/documents/uploads/pub_8984_disinformation.pdf?doc_id=2102.

[27] W.L. Bennett and S. Livingston, “The disinformation order: Disruptive communication and the decline of democratic institutions,” *European Journal of Communication*, 2018: 33(2), pp. 122-139.

This development has had far-reaching implications. For example, in the Arab world, online social networks fostered communities of individuals who shared grievances against their governments. This virtual collaboration led to plans to rise up against these governments. The ensuing uprisings resulted in a change of government in Tunisia, Libya, Egypt, Yemen, Sudan, Iraq, and political and economic concessions from the governments in Algeria, Oman, Bahrain, Morocco, and Saudi Arabia.[28] In a very real sense, without online social networks, the Arab Spring would not have occurred.

The development of mobile technologies with messaging platforms that are wifi-enabled and cellular-enabled has led to an explosion of interconnectivity. More than five billion people are estimated to own mobile devices and more than 50% of these devices are smartphones.[29] With these new technologies, individuals and groups can rapidly share content, including disinformation. This content includes messages from individuals or groups, hyperlinks to media articles, and other web content such as images and video. However, these messaging platforms may mask the identity of the sender and thus facilitate the spread of disinformation. Information shared via these messaging platforms is generally not vetted for accuracy, which makes these platforms prime candidates for exploitation by threat actors. Furthermore, end-to-end encryption on these messaging platforms can prevent the platform host from being able to moderate the content that flows through the platform.

For example, in 2017, the spread of false information led to acts of violence in India when false information about a purported gang of child kidnappers was disseminated on WhatsApp, a mobile messaging service used by over 200 million people in India.[30] Misinformation-fueled mobs killed seven people in the Indian state of Jharkhand.[31]

How Social Media Platforms Enable Disinformation Campaigns

Since the rise of social media, threat actors, whether individuals, nation-states, or other organized groups, have exploited the information environment on an unprecedented scale. Unlike the publication and distribution of print sources, which require publishing houses, editors, proofreaders, promotional advertisements, and bookstores, online information does not require an intermediary between content creator and consumer. As public confidence in mainstream media outlets has waned, interest in social media platforms and other online forums that offer uncensored communication channels to share ideas and commentary has increased. [32]

Though these platforms typically do not require payment from users in order to establish an account or access content on the platform, they are not cost-free. In exchange for granting users free access to these platforms, platform owners gather user data that enable advertisers to tailor online advertisements to known user preferences. In this arrangement, users are spared from content they have little interest in, platform owners can study user behavior to determine how to maximize the time users spend on the platform, and advertisers can serve up content more likely to engage users.

[28] Jean-Pierre Filiu. *The Arab Revolution: Ten Lessons from the Democratic Uprising*, (New York: Oxford University Press, 2011).

[29] "The Mobile Economy 2018," GSM Association, 2018, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf.

[30] Kurt Wagner, "WhatsApp Is at Risk in India. So Are Free Speech and Encryption," Vox, February 19, 2019, http://www.vox.com/2019/2/19/18224084/india-intermediary-guidelines-laws-free-speech-encryption-whatsapp.

[31] Anant R. Zanane, "WhatsApp Rumours Led To Mob Killing Of 7 In Jharkhand, Say Police," NDTV.com, May 22, 2017, https://www.ndtv.com/india-news/whatsapp-rumours-led-to-mob-killing-of-7-in-jharkhands-singhbhum-district-say-police-1696551.

[32] "Indicators of News Media," Gallup, Inc., 2018, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/216/original/KnightFoundation_Panel4_Trust_Indicators_FINAL.pdf.

The key to this system is the attention of users. The more alluring the content, the greater the time on the platform, and thus the greater the potential profit.[33] Therefore, social media platforms have an incentive to provide their users with an array of clickbait because doing so increases the revenue generated by selling online advertisements.[34]

By customizing user content, a platform effectively connects users with others who share similar views and interests. These platforms stoke the curiosity of users who want to discover what other users like them are wearing, watching, reading, and thinking.[35] The algorithms that determine what content will be displayed to individual users are designed to feed users more of what they *want* to know, not necessarily what they *should* know. The end result of this process is the creation of "echo chambers" where content inconsistent with a user's preferences fails to appear in his or her newsfeeds and other content-distribution channels.

For many people in the United States, social media platforms have become an important source of news. According to the Pew Research Center, in 2018, less than 38% of any segment of the U.S. population relied often on print newspapers.[36] Only 16% of Americans between the ages of 18 and 29 relied often on television news broadcasts; whereas 36% of this demographic group relied often on social media for news.[37] Overall, 68% of Americans get news on social media from time to time.[38] Forty-three percent (43%) of Americans get news on Facebook.[39]

The Pervasiveness of Russian Disinformation

This is why when we focus on social media effects of Russian disinfo, we completely miss the point. This is a multi dimensional, multi channel strategy, which uses different tools in complementary ways, and through which they have shaped U.S. political discourse...disinformation is often seeded at the bottom of the environment and trickles into more mainstream sites, but eventually it hits media and political influences. We can t measure the effects of disinfo through votes, but we can note where it becomes part of mainstream discourse.

Source: Kate Starbird (University of Washington), Twitter Post, July 9, 2019, 11:10 AM, https://twitter.com/katestarbird/status/1148610356895289346

The customization of content on social media platforms makes these platforms especially susceptible to disinformation campaigns.[40] Users can share information online easily and quickly, often doing so without verifying the accuracy of the shared information.[41] Although 79% of U.S. adults believe that steps should be taken to rein in fake news stories,[42] 23% have shared fake news, knowingly or unknowingly, with friends and other people online.[43] Because search algorithms provide results tied to prior online behavior, search

[33] Tim Hwang, "Digital Disinformation: A Primer," Atlantic Council, September 2017, https://www.atlanticcouncil.org/wp-content/uploads/2017/09/Digital_Disinformation_Primer_web_0925.pdf.

[34] Allcott Hunt and Matthew Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives,* vol. 31, no. 2. 2017, pp. 1–28, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

[35] Lee Ross (professor of psychology, Stanford University), in discussion with the authors, June 27, 2019.

[36] Elisa Shearer, "Social Media Outpaces Print Newspapers in the U.S. as a News Source," Pew Research Center, December 10, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

[37] Elisa Shearer, "Social Media Outpaces Print Newspapers in the U.S. as a News Source," Pew Research Center, December 10, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

[38] "News Use Across Social Media Platforms 2018," Pew Research Center, September 12, 2018, https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/.

[39] A.W. Geiger, "Key Findings about the Online News Landscape in America," Pew Research Center, September 11, 2019, https://www.pewresearch.org/fact-tank/2019/09/11/key-findings-about-the-online-news-landscape-in-america/.

[40] Paul Oliver, "The State of Disinformation on Social Media," NYU Center for Data Science, April 23, 2018, https://medium.com/center-for-data-science/the-state-of-disinformation-on-social-media-397d3c30f56a.

[41] Mike Wood, "How Does Misinformation Spread Online?," *Psychology Today*, December 6, 2018, https://www.psychologytoday.com/us/blog/web-mistrust/201812/how-does-misinformation-spread-online.

[42] Galen Stocking, "Many Americans Say Made-Up News Is A Critical Problem That Needs to Be Fixed," Pew Research Center, 5 June 2019, https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/.

[43] Denise-Marie Ordway, "Fake News and the Spread of Misinformation," Journalist's Resource, September 1, 2017, https://journalistsresource.org/studies/society/internet/fake-news-conspiracy-theories-journalism-research/.

returns will likely conform to users' preexisting biases. This content will seem more credible, at least initially, than content that flies in the face of these biases.[44] The desire of users to distinguish fake news from real news is often minimal when the news is emotionally compelling.[45] In the eyes of the user, the emotional appeal of the information may outweigh an interest in its trustworthiness.

As information is shared from user to user, the cumulative impact of this sharing may seem to render this information more legitimate due to the fact that so many users have shared it.[46] In other words, "if you make it trend, you make it true."[47] Popularity trumps accuracy.

Threat actors take advantage of the design of social media platforms and how users share information to target specific users and groups with disinformation in the hope that these users will spread this disinformation throughout the information environment. The easy transference of online information between users and platforms increases the effectiveness of modern disinformation campaigns.

During the 2016 U.S. presidential election campaign, the Internet Research Agency (IRA), based in Russia, created fake social media accounts by pretending to be U.S. citizens, operated fraudulent social media pages, and formed phony online groups all designed to attract U.S. audiences. On Twitter alone, the IRA created approximately 3,000 fake accounts that posted over 10 million tweets.[48] These accounts had over 6.4 million followers and followed 3.4 million other Twitter accounts.[49]

By capitalizing on divisive U.S. political and social issues and identifying U.S. audiences vulnerable to manipulation on social media, the IRA drew the attention of users with tantalizing content and was able to insert disinformation into the information environment where it spread rapidly and eventually metastasized to other social media platforms.[50] Mainstream news outlets, which monitored social media platforms for trending topics and reported on those topics, expanded the reach of this disinformation, highlighting how the ease of information transfer facilitates the effectiveness of modern disinformation campaigns.[51]

THE MOTIVES OF THREAT ACTORS

The sheer volume of information on the internet makes any attempt to rid the internet of inaccurate information, fake news, doctored audiovisual media, disinformation, or any other undesirable content a herculean, if not impossible, task. Therefore, government and industry leaders must focus their resources on identifying and neutralizing the greatest threats. One way to assess and prioritize threats is to identify suspected disinformation threat actors through understanding the motives for their campaigns.[52]

[44] Denise-Marie Ordway, "What Research Says about How Bad Information Spreads Online," Journalist's Resource, July 19, 2018, https://journalistsresource.org/studies/society/news-media/fake-news-bad-information-online-research/.

[45] Joe Andrews, "Fake News Is Real - A.I. Is Going to Make It Much Worse," CNBC, July 12, 2019, https://www.cnbc.com/2019/07/12/fake-news-is-real-ai-is-going-to-make-it-much-worse.html.

[46] Jon Hermann, "Defending America's National Security against Adversary ...," National Academies of Sciences, Engineering, and Medicine, accessed September 17, 2019, https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179824.pdf.

[47] Renée DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 12, 2018, https://yalereview.yale.edu/computational-propaganda.

[48] Gillian Cleary, "Twitterbots: Anatomy of a Propaganda Campaign," Symantec, June 5, 2019, https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.

[49] Gillian Cleary, "Twitterbots: Anatomy of a Propaganda Campaign," Symantec, June 5, 2019, https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.

[50] "Internet Research Agency Indictment," U.S. Department of Justice, February 16, 2018, https://www.justice.gov/file/1035477/download.

[51] Stephen Pritchard, "The Reader's Editor...reporting in haste," *The Guardian*, February 27, 2016, https://www.theguardian.com/media/2016/feb/28/the-readers-editor-on-reporting-in-haste; Casey Newton, "It's Time to End 'Trending' on Twitter," The Verge, August 13, 2019, https://www.theverge.com/interface/2019/8/13/20802974/twitter-trending-epstein-conspiracy-theories.

[52] Kaley Leetaru, "Stopping Disinformation Requires Measuring And Understanding It Not Just Monitoring And Debunking It," *Forbes*, April 27, 2019, https://www.forbes.com/sites/kalevleetaru/2019/04/27/stopping-disinformation-requires-measuring-and-understanding-it-not-just-monitoring-and-debunking-it/#57d3f1df5fd3.

Understanding why a piece of disinformation is directed at a specific audience will provide purchase on how to direct resources to negate the actor and mitigate the campaign.

Once one understands the motives of a threat actor, one may gain clarity on the objectives of specific disinformation campaigns, thus providing insight into how to neutralize the campaign and better predict the events and audiences who could be targeted in the future. The motives for disinformation campaigns are diverse and often mixed. Motivations can be financial (e.g., Macedonian threat actors' scheme to create ad revenue through incendiary content about a U.S. election[53]), political (e.g., push polling to plant false information in the minds of potential voters[54] or interest groups creating false social media content about an opponent to divide a voting bloc[55]), ideological (e.g., disagreement over a corporation's use of a social issue in its advertising, see Nike example below), legal/reputational (e.g., defense lawyers preventing reputational harm for a high-profile client and/or perpetrating harm against a defendant[56]), or a combination thereof.

The following two pages offer case studies of disinformation threat actors motivated by different factors — the first, a nation-state motivated to slow the economic and technological progress of its adversaries (Russian Promotion of 5G Dangers); the second, ideologically-motivated actors conducting a low-budget campaign to tarnish a major corporation (Campaign to Damage Nike Brand).

[53] Samanth Subramanian, "Inside the Macedonian Fake-News Complex," *Wired*, February 15, 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news/.

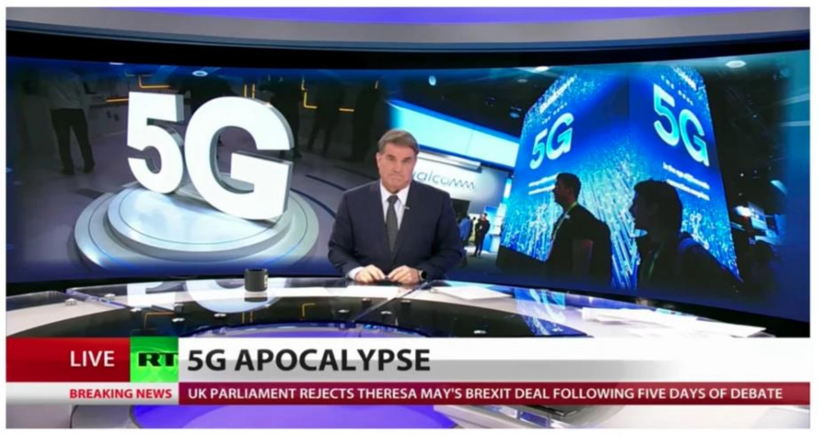
[54] Richard Gooding, "The Trashing of John McCain," *Vanity Fair*, September 24, 2008, https://www.vanityfair.com/news/2004/11/mccain200411; Jennifer Steinhauer, "Confronting Ghosts of 2000 in South Carolina," *New York Times*, October 19, 2007, https://www.nytimes.com/2007/10/19/us/politics/19mccain.html.

[55] Scott Shane and Alan Binder, "Democrats Faked Online Push to Outlaw Alcohol in Alabama Race," *New York Times*, January 7, 2019, https://www.nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html; Scott Shane and Alan Binder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *New York Times*, December 19, 2018, https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html?module=inline.

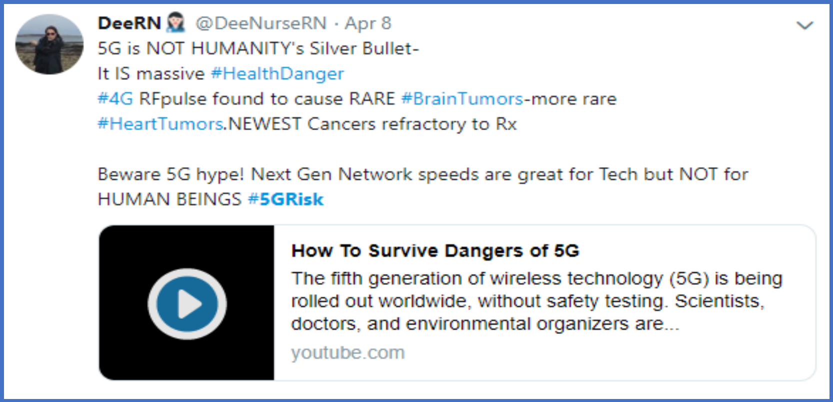
[56] Michael Barbaro, "Keeping Harvey Weinstein's Secrets, Part 1: Lisa Bloom," *New York Times*, podcast audio, September 18, 2019, https://www.nytimes.com/2019/09/18/podcasts/the-daily/harvey-weinstein-lisa-bloom.html.

RUSSIAN PROMOTION OF 5G DANGERS

Starting in 2018, Russia has supplied foreign audiences with disinformation about the supposed health dangers of 5G cellular signals. This disinformation campaign capitalizes on anxieties about radio waves causing cancer and other bodily damage.


5G
LIVE
RT
5G APOCALYPSE
BREAKING NEWS
UK PARLIAMENT REJECTS THERESA MAY'S BREXIT DEAL FOLLOWING FIVE DAYS OF DEBATE

Russia has used its RT America network to target Americans with a series of stories and news reports about the health hazards of 5G cellular signals. Inside Russia, RT reports on the scientific consensus that 5G signals promote human health; outside Russia, it reports that 5G cellular signals are more dangerous than existing 3G and 2G signals. By relying on a number of so called experts on the topic, Russia has promoted the notion that scientific controversy surrounds the issue, even though there is consensus in the scientific community that 5G signals are safe. The resulting public concern has possibly slowed the implementation of 5G technology in the West, stymied the business plans of Russia's economic competitors, and thus given Russian companies more time to establish their own 5G networks.



DeeRN 👩‍⚕️ @DeeNurseRN · Apr 8

5G is NOT HUMANITY's Silver Bullet-
It IS massive #HealthDanger
#4G RFpulse found to cause RARE #BrainTumors-more rare
#HeartTumors.NEWEST Cancers refractory to Rx

Beware 5G hype! Next Gen Network speeds are great for Tech but NOT for HUMAN BEINGS **#5GRisk**

How To Survive Dangers of 5G
The fifth generation of wireless technology (5G) is being rolled out worldwide, without safety testing. Scientists, doctors, and environmental organizers are...
youtube.com

Sources:

William Broad,   Your 5G Phone Won’t Hurt You But Russia Wants You to Think Otherwise,   *New York Times*, May 12, 2019, https://www.nytimes.com › science › 5g phone safety health russia/.

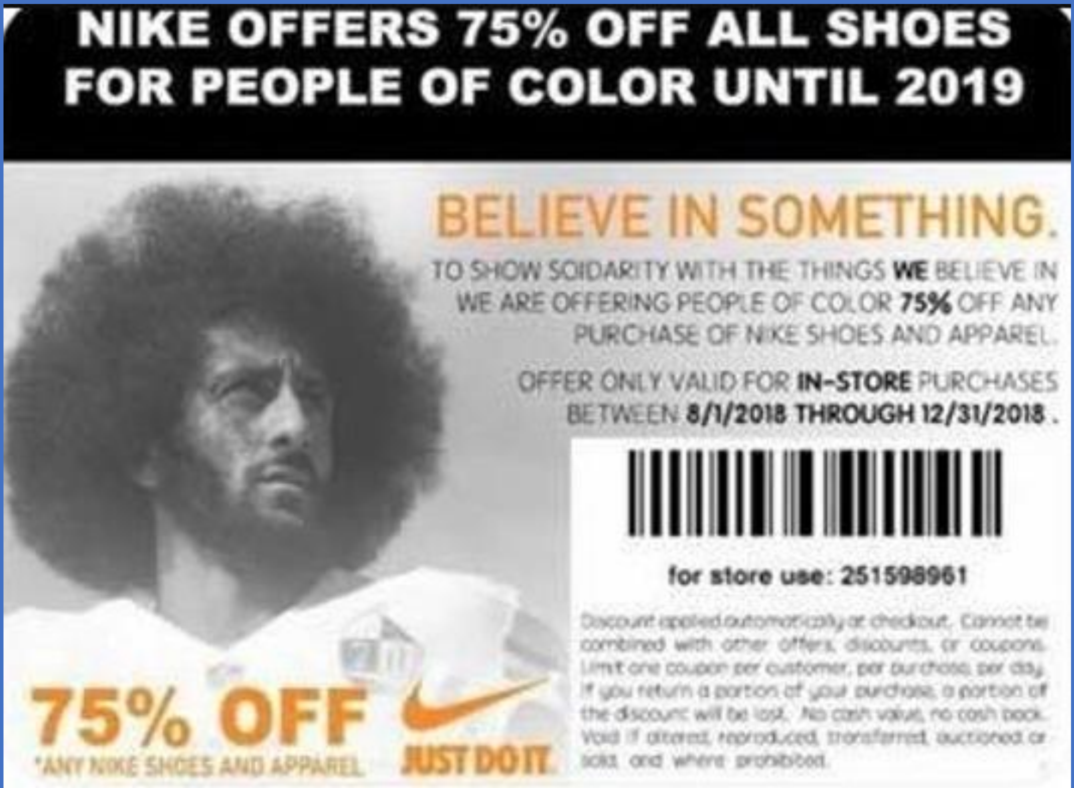
Aaron Pressman,   Health Concerns May Slow Rollout of Super Fast 5G Mobile Networks, Analyst Warns,” *Fortune*, May 22, 2019, https://fortune.com/2019/05/22/health concerns 5g cellphones cancer/.

Chris Zappone,   Russian propaganda stoking 5G health fears in Australia,   *Sydney Morning Herald*, September 16, 2019, https://www.smh.com.au/world/oceania/russian propaganda stoking 5g health fears in australia 20190916 p52rmc.html.

DeeRN, Twitter Post, April 8, 2019, 10:36 PM, https://twitter.com/DeeNurseRN/status/1115443371298967552.

CAMPAIGN TO DAMAGE NIKE BRAND

Right wing actors, unhappy about Nike's featuring of former NFL quarterback Colin Kaepernick in a 2018 advertising campaign, sought to discredit and undermine Nike's brand reputation. Kaepernick was controversial for his refusal to stand during pregame renditions of the national anthem in protest of what he saw as police brutality and systemic racism in America. After the Nike commercial aired, the disinformation threat actors created, posted, and spread fake Nike coupons featuring Kaepernick's picture and offering 75% discounts on Nike products for "people of color."



NIKE OFFERS 75% OFF ALL SHOES FOR PEOPLE OF COLOR UNTIL 2019

BELIEVE IN SOMETHING.

TO SHOW SOIDARITY WITH THE THINGS **WE** BELIEVE IN WE ARE OFFERING PEOPLE OF COLOR **75%** OFF ANY PURCHASE OF NIKE SHOES AND APPAREL.

OFFER ONLY VALID FOR **IN-STORE** PURCHASES BETWEEN **8/1/2018 THROUGH 12/31/2018**.

for store use: 251598961

Discount applied automatically at checkout. Cannot be combined with other offers, discounts, or coupons. Limit one coupon per customer, per purchase, per day. If you return a portion of your purchase, a portion of the discount will be lost. No cash value, no cash back. Void if altered, reproduced, transferred, auctioned or sold, and where prohibited.

The threat actors weaponized an existing controversy to do economic harm to a corporation with whom they disagreed. They deliberately manufactured false information (the coupon) in a low budget operation to advance a narrative that Nike is overtly political, biased, and even un American. Therefore, consumers should avoid Nike products. Although the campaign, per se, may not have done lasting damage to Nike, it shows the susceptibility of public corporations to low budget actors who can create and advance false information about an existing controversy.

Sources:

A.J. Perez, Bogus Nike Coupon featuring Colin Kaepernick offers discount to people of color, *USA Today*, September 13, 2018, https://www.usatoday.com/story/sports/nfl/2018/09/13/fake nike colin kaepernick coupon offers discount people color/1294875002/.

Misinformation vs. Disinformation: What's the difference? New Knowledge, March 7, 2019, https://www.newknowledge.com/articles/misinformation vs disinformation whats the difference/.

Attribution

Ascertaining the intent of a threat actor can be difficult if the identity of the threat actor is not known.[57] Attributing a targeted disinformation campaign to a specific threat actor is often a painstaking process.[58] Developments in technology and tactics that help mask the identity of threat actors outpace developments in technology and tactics that unmask these threat actors, especially as threat actors become more adept at exploiting authentic users.[59] The process of assessing the threat actor can be facilitated by making three preliminary determinations: (1) Is the threat actor based inside or outside the United States?; (2) Is the threat actor a nation-state, backed by a nation-state, or independent of a nation-state?; and (3) Is the purveyor of disinformation a witting or unwitting agent?

Domestic or Foreign-Based: The physical location where the disinformation originated may offer some clues as to the motives of the threat actor. A targeted disinformation campaign that originates in Mississippi whose purpose is to enflame racial tensions in the United States will have different implications than an identical campaign that originates in Tehran. Fixing the location where the disinformation originated will also help to determine which responses to the disinformation are available and which entities are best suited to respond.

State or Non-State Affiliation: State-sponsored threat actors generally have more resources available to conduct disinformation campaigns than threat actors not backed by nation-states and therefore the resources to sustain and protect these campaigns over an extended period of time. Different tools are available to respond to the actions of nation-states, as opposed to the actions of non-state actors. The former is a matter of international relations and national security; the latter may be best addressed through the criminal justice system.

Witting or Unwitting Agents: Threat actors are witting purveyors of disinformation—people or entities directly supporting a disinformation campaign and aware of the campaign's malign motives. Threat actors should be distinguished from unwitting agents, people or entities supporting a disinformation campaign while unaware of the malign motives underlying the campaign. A "useful idiot" is a type of unwitting agent who is perceived to be sympathetic to the actor's cause, but does not comprehend the objectives of the campaign. Unwitting agents often spread disinformation not knowing that he or she is participating in a disinformation campaign. Responses to the different threat actors will vary depending on their level of intentional involvement in the targeted disinformation campaign.

The Role of Bots in Disinformation Campaigns

Threat actors can amplify disinformation through the use of bot networks, social media followers, or pre-established accounts. Bots are computer algorithms designed to execute specific online tasks autonomously and repetitively.[60] They simulate the behavior of human beings in social networks, interacting with other

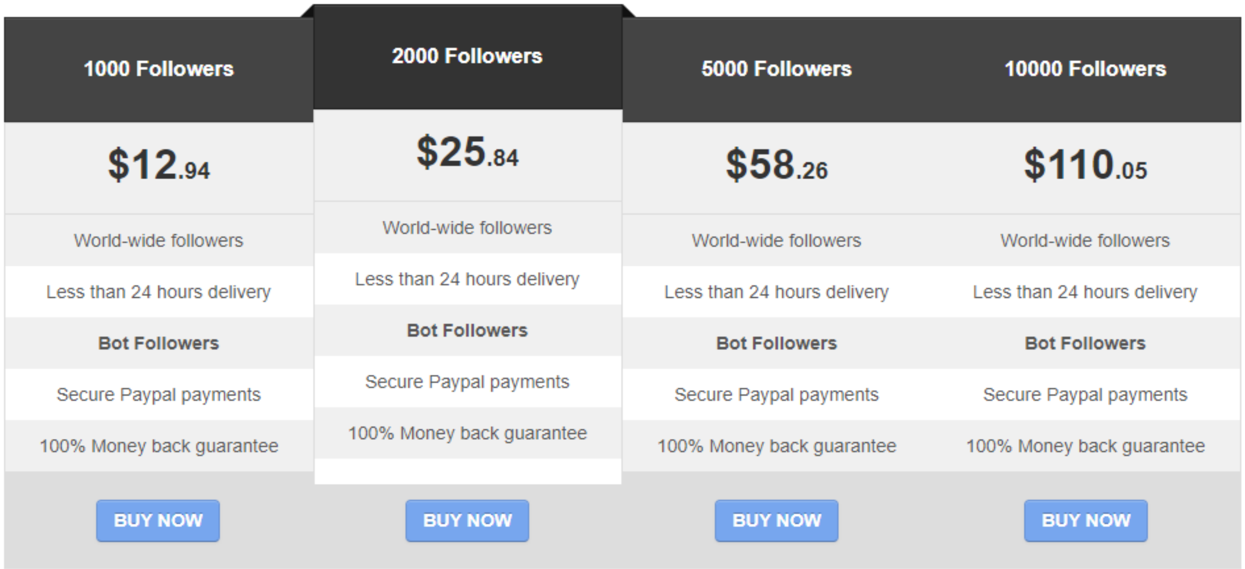
[57] Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data & Society, May 15, 2017, https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

[58] David E. Sanger, Jim Rutenberg, and Eric Lipton. "Tracing Guccifer 2.0's Many Tentacles in the 2016 Election." *New York Times*, July 15, 2018, https://www.nytimes.com/2018/07/15/us/politics/guccifer-russia-mueller.html.

[59] Elizabeth Bodine-Baron, Todd C Helmus, Todd C., Andrew Radin, and Elina Treyger, "Countering Russian Social Media Influence," RAND Corporation, 2018, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf.

[60] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019, https://www.cits.ucsb.edu/fake-news/spread.

users and sharing information and messages.[61] Millions of bots spread information on social media platforms such as Facebook, Twitter, and Instagram. According to a 2017 estimate, there were 23 million bots on Twitter (around 8.5% of all Twitter accounts), 140 million bots on Facebook (up to 5.5% of all Facebook accounts) and approximately 27 million bots on Instagram (8.2% of all Instagram accounts).[62] These three platforms alone contained 190 million bots—more than half the number of people who live in the entire United States.[63] These zombie-like accounts often sit dormant, waiting for external activation to begin their preassigned tasks on the platform. Bot accounts are advertised and sold legally on a number of websites. See the table below for an example of publicly available plans to purchase bots.



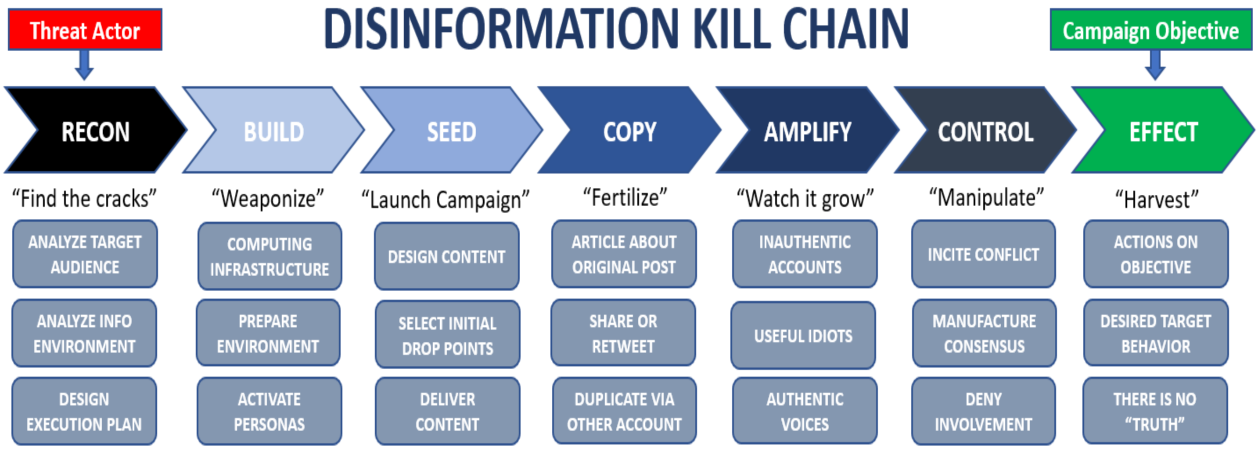
1000 Followers	2000 Followers	5000 Followers	10000 Followers
$12.94	$25.84	$58.26	$110.05
World-wide followers	World-wide followers	World-wide followers	World-wide followers
Less than 24 hours delivery	Less than 24 hours delivery	Less than 24 hours delivery	Less than 24 hours delivery
Bot Followers	Bot Followers	Bot Followers	Bot Followers
Secure Paypal payments	Secure Paypal payments	Secure Paypal payments	Secure Paypal payments
100% Money back guarantee	100% Money back guarantee	100% Money back guarantee	100% Money back guarantee
BUY NOW	BUY NOW	BUY NOW	BUY NOW

Source: "Fake Twitter Followers (Bots)," CompraSocialMedia.com, accessed September 19, 2019, https://www.compra-seguidores.com/en/buy-fake-followers/.

DISINFORMATION KILL CHAIN

The "connectedness" of modern society and the free availability of content distribution platforms has greatly increased the scope, scale, and speed of disinformation campaigns. Disinformation campaigns are not a new phenomenon. While the scale of attack, scope of impact, and speed of execution of modern disinformation campaigns have brought new attention to the issue, the fundamental elements of such campaigns pre-date the internet. The cyber kill chain model[64] serves as an inspiration for the following framework, which outlines the basic structure of these campaigns.

[61] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019, https://www.cits.ucsb.edu/fake-news/spread.
[62] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019. https://www.cits.ucsb.edu/fake-news/spread.
[63] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019. https://www.cits.ucsb.edu/fake-news/spread.
[64] *The Cyber Kill Chain*®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

Campaign objective: A threat actor starts with an objective, such as changing a population's opinion on a topic (Brexit, war in Syria, Hong Kong protesters), steering voters toward a preferred candidate, or offering a counternarrative to the status quo.

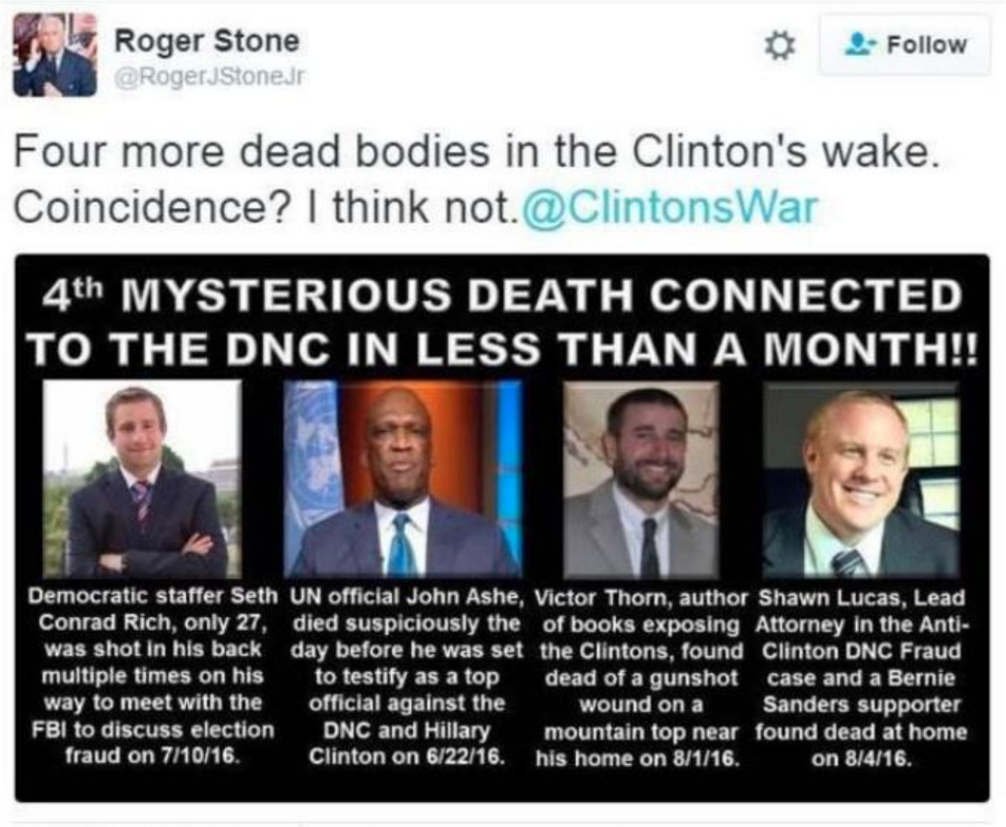
1. Reconnaissance: Analyze target audience and how information flows through the target's environment, identify societal fissures to exploit, and design campaign execution plan.
2. Build: Build campaign infrastructure (computing resources, operational staff, initial accounts, personas, bots, and websites). Sophisticated threat actors may prepare the environment through tailored diplomatic, propaganda, and/or official messaging.
3. Seed: Create fake and/or misleading content, then launch campaign by delivering content to initial seeding locations such as online forums or social media platforms. Delivering content to multiple locations using different accounts can create the illusion that there are multiple sources for a story.
4. Copy: Write articles, blogs, and/or new social media posts referencing the original story. Witting agents can assist by using their media platforms for seemingly authentic distribution. The copy phase is a form of "information laundering," laying the groundwork for amplification by adding legitimacy to poorly sourced stories.
5. Amplify: Amplify content by pushing the story into the communication channels of the target audience. The use of bots and inauthentic accounts help provide momentum, then the content may be distributed by other witting agents (quasi-legitimate journalists) and unwitting agents (useful idiots). Successful amplification will result in the content being distributed by authentic voices, such as the mainstream media, which provides a trending effect and subsequent amplification by other unwitting agents and the target audience (i.e., now the unwitting audience is spreading misinformation because they do not know it is false and want to be helpful by informing their peers).
6. Control: Control the effect and manipulate the target's reaction by infiltrating conversations about the content. Incite conflict and/or strengthen the illusion of consensus by trolling comment sections of online posts. If a threat actor is accused of propagating disinformation, he or she may deny it vehemently, offer a counternarrative, and/or accuse an opposing party of planting the story.
7. Effect: Target actualizes the desired effect, such as voting for a preferred candidate, expressing behavior against a preferred group, or losing faith in the very idea of truth.

A threat actor may skip steps in this process, but doing so can reduce the effectiveness of the campaign and make it more difficult to mask the identity and objectives of the threat actor. Well-resourced threat actors may support and enable their campaigns through use of the entire influence toolkit, including economic and diplomatic activities, public relations, and espionage.

Case Studies

Below are two examples of disinformation campaigns executed by state-sponsored threat actors, which illustrate the phases of the disinformation kill chain.

In the first example, a fake story about the purported political assassination of Seth Rich, an employee of the Democratic National Committee (DNC), made its way from a Russian propaganda and conspiracy website, through Fox News, and into mainstream American discourse. It is important to note that Seth Rich's murder has remained unsolved, but no evidence has emerged which suggests that his death was a political assassination. The Rich family sued Fox News for "intentional infliction of emotional distress."[65] Fox News later retracted the article, saying "the article was not initially subjected to the high degree of editorial scrutiny we require for all our reporting."[66] Despite the retraction, high-profile Fox News personalities continued to discuss the conspiracy. After it trended, it was "true." Examples of content from the Seth Rich conspiracy are followed by an outline of the campaign (note the involvement of Russia's UK Embassy):



Roger Stone
@RogerJStoneJr

Four more dead bodies in the Clinton's wake. Coincidence? I think not.@ClintonsWar

4th MYSTERIOUS DEATH CONNECTED TO THE DNC IN LESS THAN A MONTH!!

Democratic staffer Seth Conrad Rich, only 27, was shot in his back multiple times on his way to meet with the FBI to discuss election fraud on 7/10/16.

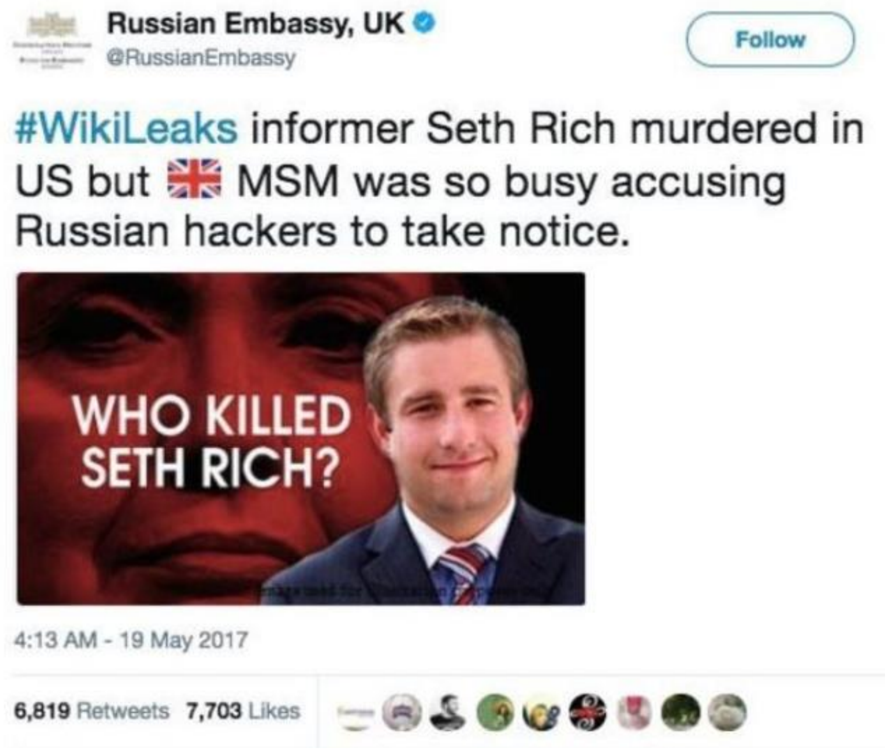
UN official John Ashe, died suspiciously the day before he was set to testify as a top official against the DNC and Hillary Clinton on 6/22/16.

Victor Thorn, author of books exposing the Clintons, found dead of a gunshot wound on a mountain top near his home on 8/1/16.

Shawn Lucas, Lead Attorney in the Anti-Clinton DNC Fraud case and a Bernie Sanders supporter found dead at home on 8/4/16.

[65] Avie Schneider, "Appeals Court Reinstates Lawsuit Against Fox News Over Seth Rich Story," NPR, September 13, 2019, https://www.npr.org/2019/09/13/760681773/appeals-court-reinstates-lawsuit-against-fox-news-over-seth-rich-story.

[66] "Statement on coverage of Seth Rich murder investigation," Fox News, May 23, 2017, https://www.foxnews.com/politics/statement-on-coverage-of-seth-rich-murder-investigation.

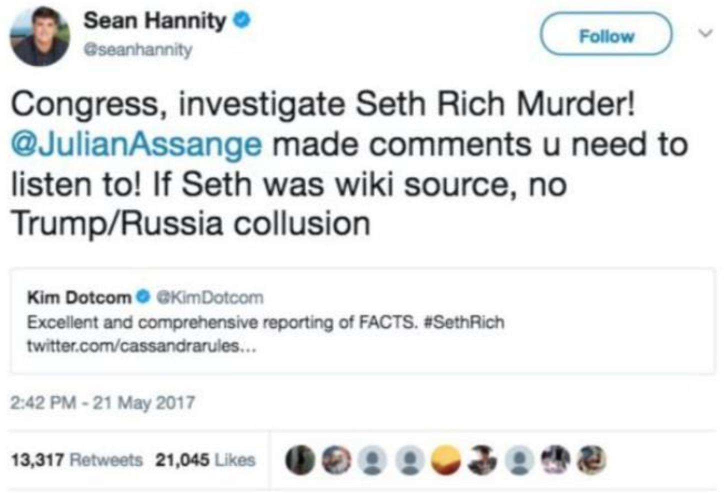


Russian Embassy, UK
@RussianEmbassy

#WikiLeaks informer Seth Rich murdered in US but 🇬🇧 MSM was so busy accusing Russian hackers to take notice.

4:13 AM - 19 May 2017

6,819 Retweets 7,703 Likes



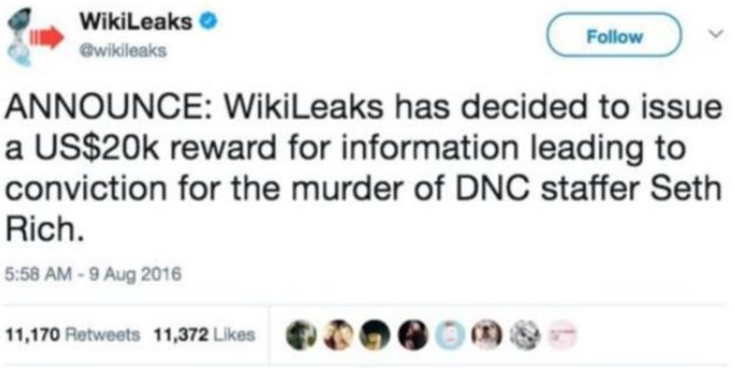
Sean Hannity
@seanhannity

Congress, investigate Seth Rich Murder! @JulianAssange made comments u need to listen to! If Seth was wiki source, no Trump/Russia collusion

Kim Dotcom @KimDotcom
Excellent and comprehensive reporting of FACTS. #SethRich
twitter.com/cassandrarules...

2:42 PM - 21 May 2017

13,317 Retweets 21,045 Likes



WikiLeaks
@wikileaks

ANNOUNCE: WikiLeaks has decided to issue a US$20k reward for information leading to conviction for the murder of DNC staffer Seth Rich.

5:58 AM - 9 Aug 2016

11,170 Retweets 11,372 Likes

CASE STUDY Seth Rich Murder (2016)		THREAT ACTOR Russian Foreign Intelligence Service (SVR)	
AFFILIATION State-sponsored	TARGET AUDIENCE US population	OBJECTIVE Counternarrative: Deflect special counsel investigation; if Seth Rich leaked the emails, then Russia wasn't involved with the DNC hack	MOTIVE Political
NARRATIVE	Seth Rich was a staffer for the Democratic National Committee; he leaked DNC emails to Wikileaks and planned to report wrongdoing by the Hillary Clinton campaign to the FBI; Clinton-affiliated assassins murdered him.		
PHASE	PRIMARY PLATFORM	PHASE DESCRIPTION	AGENTS
Seed	SVR bulletin; whatdoesitmean.com	SVR circulates ficticious intel report about the murder; citing "Russian intelligence," an article is published to an obscure website suggesting Rich was murdered by Clinton assassins; website is known source for Russian propaganda	threat actor
Copy	Reddit; alt-right sites; Twitter; RT; Sputnik	Rich conspiracy story posted on Reddit and Twitter	threat actor; witting agents; unwitting agents
Amplify	Twitter; Facebook; YouTube; Infowars; America First Media; Fox News	IRA bots repost story en masse; witting and unwitting agents retweet; alt-right websites aggressively push the story; Fox News picks it up and amplifies to mainstream US audiences	threat actor (bots); witting agents; unwitting agents
Control	Twitter comments; Fox News; YouTube; alt-right sites; RT; Sputnik	Bots & trolls infiltrate organic online conversations discussing the story to sow divisions; Julian Assange suggests Seth Rich was source for Wikileaks; Fox News continues to push the story; after Yahoo News report about SVR as source of conspiracy, a new disinformation effort begins to counter that narrative	threat actor (bots & trolls); witting agents; unwitting agents

Sources:

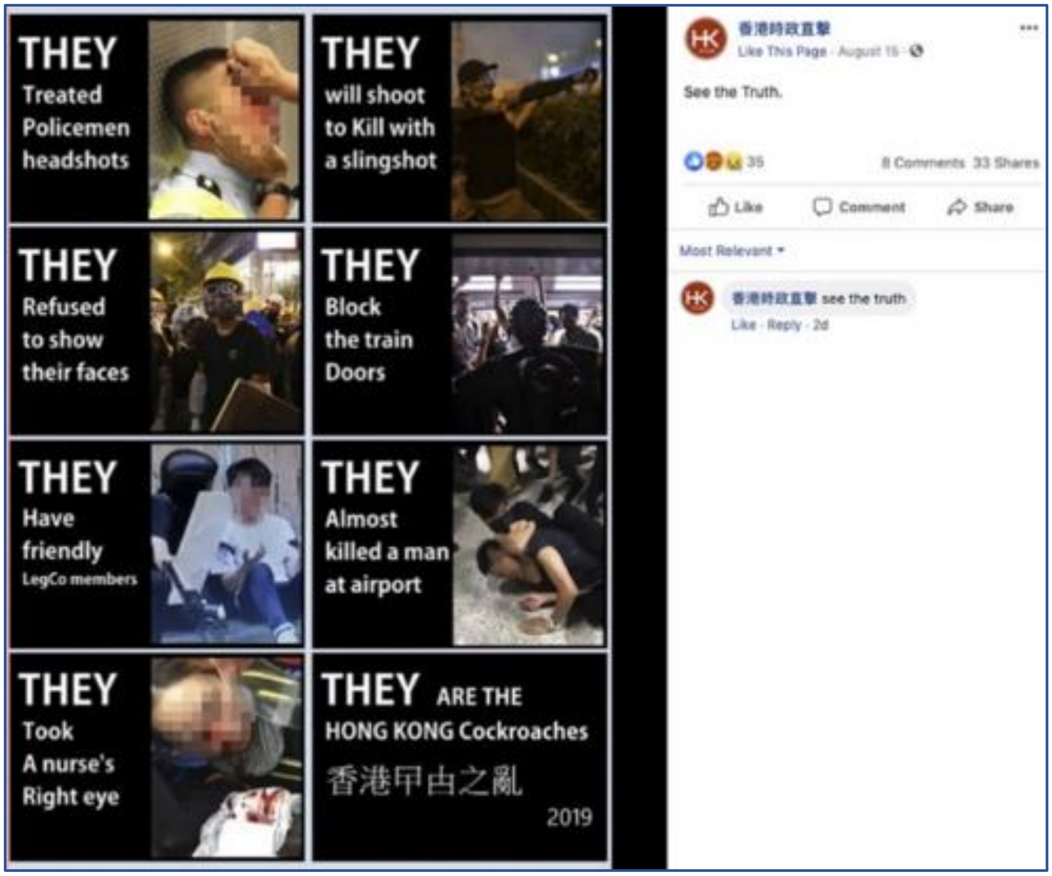
Michael Isikoff, "Exclusive: The true origins of the Seth Rich conspiracy theory. A Yahoo News Investigation," Yahoo News, July 9, 2019, https://news.yahoo.com/exclusive-the-true-origins-of-the-seth-rich-conspiracy-a-yahoo-news-investigation-100000831.html.

Charlie Mole, "Seth Rich: How a young man's murder attracted conspiracy theories," BBC News, April 21, 2018, https://www.bbc.com/news/blogs-trending-43727858.

The second example is the disinformation campaign launched against protestors in Hong Kong in 2019. Facebook and Twitter revealed that they had removed or suspended over 200,000 fraudulent accounts that were circulating information to discredit individuals and groups that had been protesting against the extradition bill pending in the Legislative Council of Hong Kong.[67] This campaign, sponsored by the Chinese government, sought to discredit the protestors and the larger pro-democracy movement in Hong Kong. The fraudulent accounts, some of which claimed to be users with American identities, pushed narratives praising the police and depicting the protestors in Hong Kong as cockroaches and terrorists.[68] The following are two disinformation items used in the campaign against the Hong Kong protests.

[67] Kari Paul, "Twitter and Facebook Crack down on Accounts Linked to Chinese Campaign against Hong Kong," *The Guardian*, August 19, 2019, https://www.theguardian.com/technology/2019/aug/19/twitter-china-hong-kong-accounts.

[68] Marie C. Baca and Tony Romm, "Twitter and Facebook Take First Actions against China for Using Fake Accounts to Sow Discord in Hong Kong," *Washington Post*, August 19, 2019, https://www.washingtonpost.com/technology/2019/08/19/twitter-suspends-accounts-it-accuses-china-coordinating-against-hong-kong-protesters/.


THEY Treated Policemen headshots
THEY will shoot to Kill with a slingshot
THEY Refused to show their faces
THEY Block the train Doors
THEY Have friendly LegCo members
THEY Almost killed a man at airport
THEY Took A nurse's Right eye
THEY ARE THE HONG KONG Cockroaches
香港甲由之亂
2019

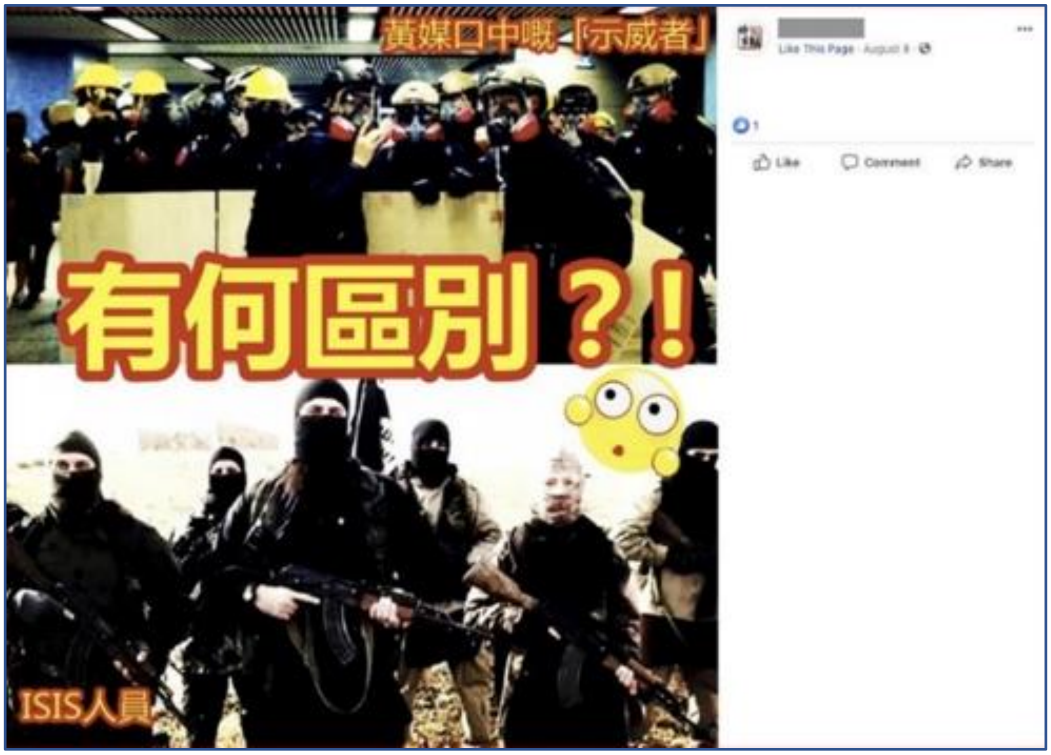
香港時政直擊
Like This Page · August 15 ·

See the Truth.

35 · 8 Comments 33 Shares

Like
Comment
Share
Most Relevant

香港時政直擊 see the truth
Like · Reply · 2d



[redacted]
Like This Page · August 8 ·

1

Source: Kate Conger, “Facebook and Twitter Say China Is Spreading Disinformation in Hong Kong,” *New York Times*, August 19, 2019, https://www.nytimes.com/2019/08/19/technology/hong-kong-protests-china-disinformation-facebook-twitter.html.

CASE STUDY Hong Kong 2019 Protests		THREAT ACTOR Chinese Government	
AFFILIATION State-sponsored	TARGET AUDIENCE Worldwide Audience	OBJECTIVE Discredit the Pro-Democracy Movement	MOTIVE Political
NARRATIVE	Individuals protesting the previously proposed extradition bill in Hong Kong bill are not credible and destructive to China.		
PHASE	PRIMARY PLATFORM	PHASE DESCRIPTION	AGENTS
Seed	Facebook, Twitter	Set up fake profiles as Americans from Nevada, Ohio, and Texas with mainstream conservative views.	Chinese government; witting agents
Copy	Facebook, Twitter	Create approximately 20,000 additional accounts to propogate similar information across platforms	witting agents; unwitting agents
Amplify	Twitter, Facebook, including paid advertisements from Chinese state-run media (China Daily, Xinhua News, and CGTN)	Bots and other user accounts repost story en masse; witting and unwitting agents retweet	witting agents; unwitting agents
Control	Facebook, Twitter	In response to the campaign, Twitter and Facebook shut down thousands of accounts. Twitter closed nearly 1,000 active accounts that were part of the operation and roughly 200,000 it said amplified and supported the campaign. Facebook closed five accounts, seven pages and three groups on its platform. Facebook said that the pages it removed had about 15,500 accounts following one or more pages, while 2,200 accounts joined at least one of the groups.	Chinese government (bots & trolls); witting agents; unwitting agents

Sources: Marie C. Baca and Tony Romm, "Twitter and Facebook Take First Actions against China for Using Fake Accounts to Sow Discord in Hong Kong," *Washington Post*, August 19, 2019, https://www.washingtonpost.com/technology/2019/08/19/twitter-suspends-accounts-it-accuses-china-coordinating-against-hong-kong-protesters/.

Craig Timberg, Drew Harwell and Tony Romm, "In accusing China of disinformation, Twitter and Facebook take on a role they've long rejected," *Washington Post*, August 20, 201,. https://www.washingtonpost.com/technology/2019/08/20/after-twitter-facebook-blame-china-hong-kong-disinformation-government-defends-its-right-online-speech/?noredirect=o.

Louise Matsakis, "China Attacks Hong Kong Protesters with Fake Social Posts," *Wired*, August 19 2019, https://www.wired.com/story/china-twitter-facebook-hong-kong-protests-disinformation/.

COMBATTING THE ISSUE

The rapid pace of innovations on social media platforms, the shifting tastes of users who skip from one platform to another, and the immense array of content on social media, and comparable forums make it extremely challenging for government entities and platform owners to monitor and regulate inauthentic behavior. Since no government or platform owner has unlimited resources to devote to combatting disinformation campaigns, the amount of effort and resources required to keep pace with ongoing campaigns detracts from the capacity to develop strategies and technology that might prevent future disinformation campaigns or mitigate the damage these campaigns might cause. Before turning to a response framework to combat disinformation campaigns, we will review current efforts by some of the major stakeholders.

Social Media Platforms

While some major social media platforms have taken steps to limit disinformation on their platforms, these steps, in general, have been reactive in nature. The use of third-party fact checkers and the development of techniques to detect inauthentic accounts are examples of such steps.[69] During elections, Facebook has established "war rooms" to identify and respond to disinformation found on the platform.[70] Google has committed to sharing information concerning disinformation campaigns with law enforcement and other platforms when encountered.[71] However, these platforms are currently fighting a losing battle. As soon as one disinformation campaign is dismantled or inauthentic account deleted, another rears its ugly head, forcing the platforms to engage in a perpetual game of "whack-a-mole".

Social media platforms are also implementing more proactive measures to combat disinformation campaigns. Facebook and Instagram now permit organizations, which buy political ads or issue-oriented ads on these platforms, to run these ads only under the identities that the platform has first verified.[72]

Following the takedown of the Hong Kong protest disinformation campaign described above, Twitter updated its advertising policies whereby it "will not accept advertising from state-controlled news media entities. Any affected accounts will be free to continue to use Twitter to engage in public conversation, just not our advertising products."[73] Since social media platforms have a financial incentive to permit content that attracts user attention, whether factual or false, they are unlikely without external pressure to fundamentally adjust their business models.[74]

Government

In many respects, government entities have a far more powerful and extensive arsenal with which to combat targeted disinformation campaigns than social media companies. Governments can impose economic sanctions and civil fines, arrest and prosecute, limit international travel, seize websites, and withdraw tax-exempt status. Governments can also attempt to pressure social media companies to modify their practices by exposing these practices to public scrutiny.[75] However, constitutional and other legal guarantees of free speech constrain government efforts to regulate the content of online information.

The U.S. government's approach to combatting disinformation campaigns includes the establishment of special units whose focus is to counter foreign influence and share threat information with the private sector. Additionally, there is growing support for amending Section 230 of the Communications Decency Act, which could potentially make social media platforms civilly liable for content that users post on these platforms.

[69] "Working to Stop Misinformation and False News," Facebook, April 7, 2017, http://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news.

[70] Davey Alba, "Facebook Tightens Rules on Verifying Political Advertisers," *New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/technology/facebook-election-advertising-disinformation.html.

[71] Salvador Rodriguez, "The FBI Visits Facebook to Talk about 2020 Election Security, with Google, Microsoft and Twitter Joining," CNBC, September 5, 201, https://www.cnbc.com/2019/09/04/facebook-twitter-google-are-meeting-with-us-officials-to-discuss-2020-election-security.html.

[72] Nancy Scola, "Facebook Revamps Election Ad Rules amid Disinformation Fears," POLITICO, August 28, 2019, https://www.politico.com/story/2019/08/28/facebook-election-ad-rules-disinformation-1476638.

[73] "Information Operations Directed at Hong Kong," Twitter, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html; "Updating Our Advertising Policies on State Media," Twitter, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.

[74] Michael Posner, "How Social Media Companies Need To Address Disinformation Globally," *Forbes*, June 16, 2019, https://www.forbes.com/sites/michaelposner/2019/06/16/how-social-media-companies-need-to-address-disinformation-globally/#2d2e178e3f9f.

[75] Douglas Soule, "US Falls Behind EU in Responding to Disinformation Campaign," The Globe Post, August 3, 2019, https://theglobepost.com/2019/08/03/us-eu-disinformation-response/.

Citizenry

The brunt of the effort to combat disinformation campaigns ultimately falls on the users of social media platforms and other online forums. Without users willing to endorse and share disinformation, disinformation campaigns would be deprived of the fuel that powers them – "We have met the enemy and he is us."[76] Some researchers have likened the problem of making users less vulnerable to disinformation to inoculating a population against disease, suggesting that disinformation can infect a population similar to a virus.[77] Media literacy campaigns can be an effective means of inoculating users against the disease of disinformation. The U.S.-based National Association for Media Literacy Education defines media literacy as "the ability to access, analyze, evaluate, create, and act using all forms of communication…Media literacy empowers people to be critical thinkers, effective communicators, and active citizens."[78]

There are indications that the American public sense the need to become more media literate. Studies indicate that news consumers had difficulty distinguishing between real news and disinformation during the 2016 U.S. presidential election.[79] These consumers thought accuracy, impartiality, and transparency were the most important factors in trusting news sources, and they want news organizations to do a more thorough job of vetting information on their websites and to provide more ready access to fact-checking resources.[80]

RESPONSE FRAMEWORK

Mitigating the threat posed by sophisticated disinformation threat actors requires a whole-of-society response. Our recommendations revolve around three themes: hit the actor, hit the technology, and build public resilience. Fundamental to these themes is a culture of shared responsibility and a framework to share threat information across stakeholders in a way that protects the privacy of social media users.

Hit the Actor

Government Stakeholders:

- Move aggressively to collect information regarding the order of battle, objectives, tactics, techniques, and procedures of disinformation threat actors;
- Hold those actors accountable through a comprehensive approach involving diplomatic pressure, adversary engagement, criminal indictments, and daylighting their malign activities;
- Develop a prioritized list of events disinformation threat actors are likely to target (elections, political events, military exercises, census, etc.) and convene "war rooms" to bring together appropriate public and private sector stakeholders to combat disinformation in real time.

[76] Thomas Fingar (Shorenstein APARC Fellow in the Freeman Spogli Institute for International Studies, Stanford University), quoting the Pogo comic strip from 1971 in discussion with the authors, June 28, 2019.

[77] Jon Roozenbeek and Sander van der Linden, "The Fake News Game: Actively Inoculating Against the Risk of Misinformation," accessed September 17, 2019, https://www.cam.ac.uk/sites/www.cam.ac.uk/files/fakenews_latest_jrr_aaas.pdf.

[78] "Media Literacy Defined," National Association for Media Literacy Education, accessed September 17, 2019, https://namle.net/publications/media-literacy-definitions/.

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

[80] "Indicators of News Media Trust," Knight Foundation, September 11, 2018, https://www.knightfoundation.org/reports/indicators-of-news-media-trust.

Social Media Platforms:

- Improve disinformation discovery tools and promptly take down the threat actor's infrastructure upon discovery;
- Share relevant signatures of disinformation campaigns with other platforms;
- De-emphasize content promulgated by overt authoritarian state-sponsored organizations. Further prohibit political advertisement by such organizations.

Academia and Civil Society Researchers: Continue investigating active disinformation campaigns across the information environment and analyze past campaigns to better understand the threat actors, their motives, and their techniques.

Hit the Technology

Government Stakeholders: Continue funding research for the development of technical tools to identify disinformation campaign signatures across platforms, including coordinated inauthentic behavior (e.g., creation of false personas, creation of fraudulent groups and websites, deployment of bots and trolls, and other suspicious account activity) and associated inauthentic content (e.g., fake or manipulated video, audio, images, text, and documents).

Industry and Academia: Design, build, and sell technical tools to identify and analyze disinformation campaigns across platforms.

Social Media Platforms: Employ technical tools to rapidly identify and analyze disinformation campaigns.

Build Resilience

Educational Institutions: Educational programs, from primary through graduate level, should integrate media literacy into their curricula. Increased media literacy across society would build resilience in the face of disinformation attacks, hardening the nation's defenses against both foreign and domestic disinformation actors. Media literacy and mature information consumption could be framed as a patriotic choice in defense of democracy.

Advocacy Groups: Advocacy and special interest groups (AARP, NAACP, Veterans of Foreign Wars, etc.) should promulgate media literacy information through their information distribution channels in a format tailored to their membership (e.g., The War on Pineapple).[81]

Government Stakeholders:

- *Transparency* – Legislation should emphasize the importance of content transparency and authenticity. Follow through on Honest Ads Act proposed in the U.S. Senate, which currently has bipartisan support. The act would amend the 1971 definition of "electioneering communication" to include internet-based political advertising, making internet-based ads subject to the same disclosure requirements as television, radio, and print media.
- *Literacy* – Fund research investigating the impact of disinformation campaigns across demographics and effective methods for providing media literacy education to those demographics.

[81] Department of Homeland Security, "The War on Pineapple: Understanding Foreign Interference in 5 Step," Cybersecurity and Infrastructure Security Agency, June 2019, https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf.

Academia and Civil Society Researchers:

- *Transparency* – Continue investigating the methods and technical means to provide transparency to the source of online content, such as a "nutrition label" for content providers (i.e. the Trust Project).[82]
- *Literacy* – Conduct media literacy research to identify trends in susceptibility to disinformation across demographics, the negative impact of disinformation campaigns, and approaches to providing media literacy education to susceptible populations.

Social Media Platforms:

- *Transparency* – Provide transparency regarding the geographic location of organizational page owners, history of name changes for the page, and apply "nutrition label" type information for organizational content providers.
- *Literacy* – Make readily available for users information about the platform's policies on disinformation and provide educational material about the judicious consumption of information online.

News Media Organizations:

- *Transparency* – Provide transparency regarding the source, author, and/or producer of news content, including their expertise, funding, conflicts of interest, and agenda. This information should be embedded with content and easily discoverable by consumers. News media organizations should strive to meet journalism standards of trustworthiness, such as citing sources, correcting mistakes, and avoiding conflicts of interest and political bias. Apply a news content "nutrition label" or Trust Mark[83] so consumers are aware of any explicit bias.

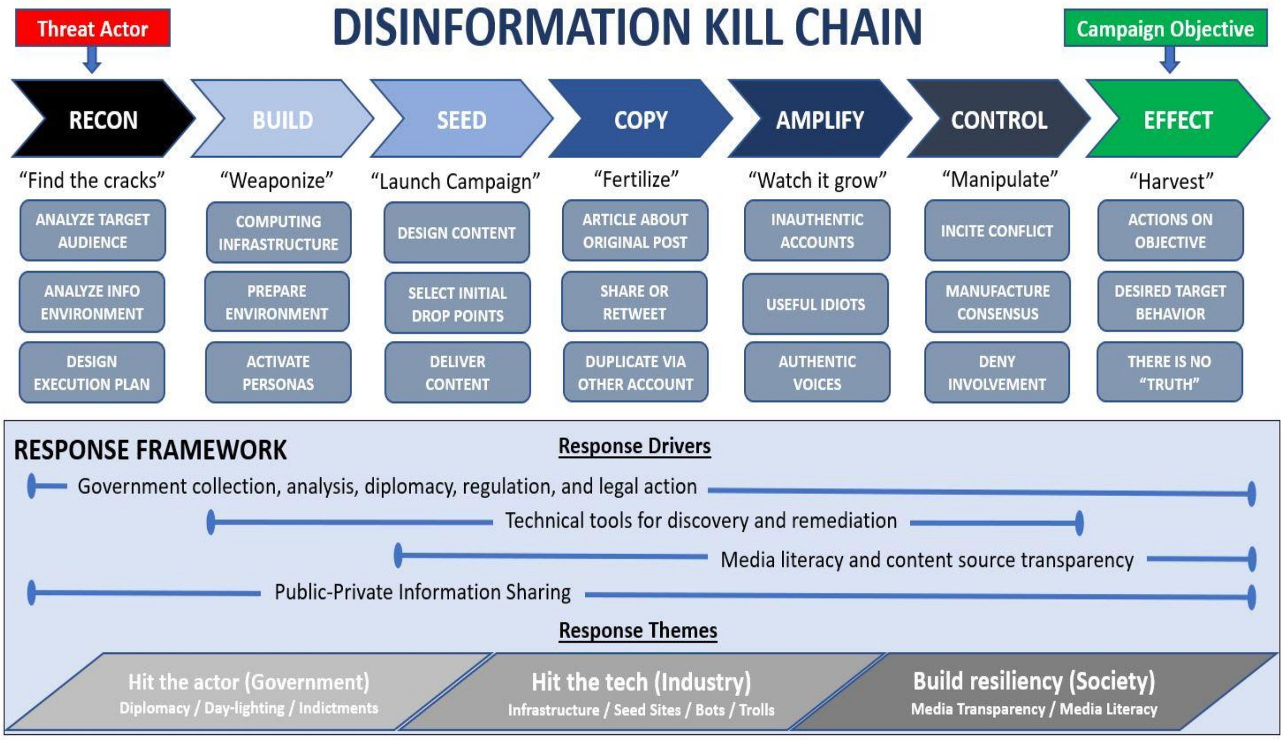
Information Sharing

An information sharing and analysis organization should be established with members from social media companies, research institutions, and news media organizations with the following objectives:

1. Establish a repository of social media data accessible to vetted researchers. Data stored and shared in a way that ensures user privacy (a trusted third party may act as gatekeeper);
2. Provide a framework for cross-platform analysis of disinformation campaigns to better understand threat actors, their tactics, and the impact of their activities;
3. Promote the advancement of methodologies, technical tools, and strategies for detecting disinformation, neutralizing threat actors, and reducing the negative impact of disinformation;
4. Facilitate information exchange between the federal government (appoint government lead responsible for disinformation issues) and social media companies;
5. Provide a process for sharing real-time threat information in a way that ensures user privacy.

[82] "What Is the Trust Project and What Does It Do?," The Trust Project, accessed September 17, 2019, https://thetrustproject.org/faq/#what_does_it_do.

[83] "What Is the 'Trust Mark'?," The Trust Project, accessed September 17, 2019, https://thetrustproject.org/faq/#trust_mark.



Threat Actor

DISINFORMATION KILL CHAIN

Campaign Objective

RECON — "Find the cracks"
- ANALYZE TARGET AUDIENCE
- ANALYZE INFO ENVIRONMENT
- DESIGN EXECUTION PLAN

BUILD — "Weaponize"
- COMPUTING INFRASTRUCTURE
- PREPARE ENVIRONMENT
- ACTIVATE PERSONAS

SEED — "Launch Campaign"
- DESIGN CONTENT
- SELECT INITIAL DROP POINTS
- DELIVER CONTENT

COPY — "Fertilize"
- ARTICLE ABOUT ORIGINAL POST
- SHARE OR RETWEET
- DUPLICATE VIA OTHER ACCOUNT

AMPLIFY — "Watch it grow"
- INAUTHENTIC ACCOUNTS
- USEFUL IDIOTS
- AUTHENTIC VOICES

CONTROL — "Manipulate"
- INCITE CONFLICT
- MANUFACTURE CONSENSUS
- DENY INVOLVEMENT

EFFECT — "Harvest"
- ACTIONS ON OBJECTIVE
- DESIRED TARGET BEHAVIOR
- THERE IS NO "TRUTH"

RESPONSE FRAMEWORK

Response Drivers

Government collection, analysis, diplomacy, regulation, and legal action

Technical tools for discovery and remediation

Media literacy and content source transparency

Public-Private Information Sharing

Response Themes

Hit the actor (Government) — Diplomacy / Day-lighting / Indictments

Hit the tech (Industry) — Infrastructure / Seed Sites / Bots / Trolls

Build resiliency (Society) — Media Transparency / Media Literacy

Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

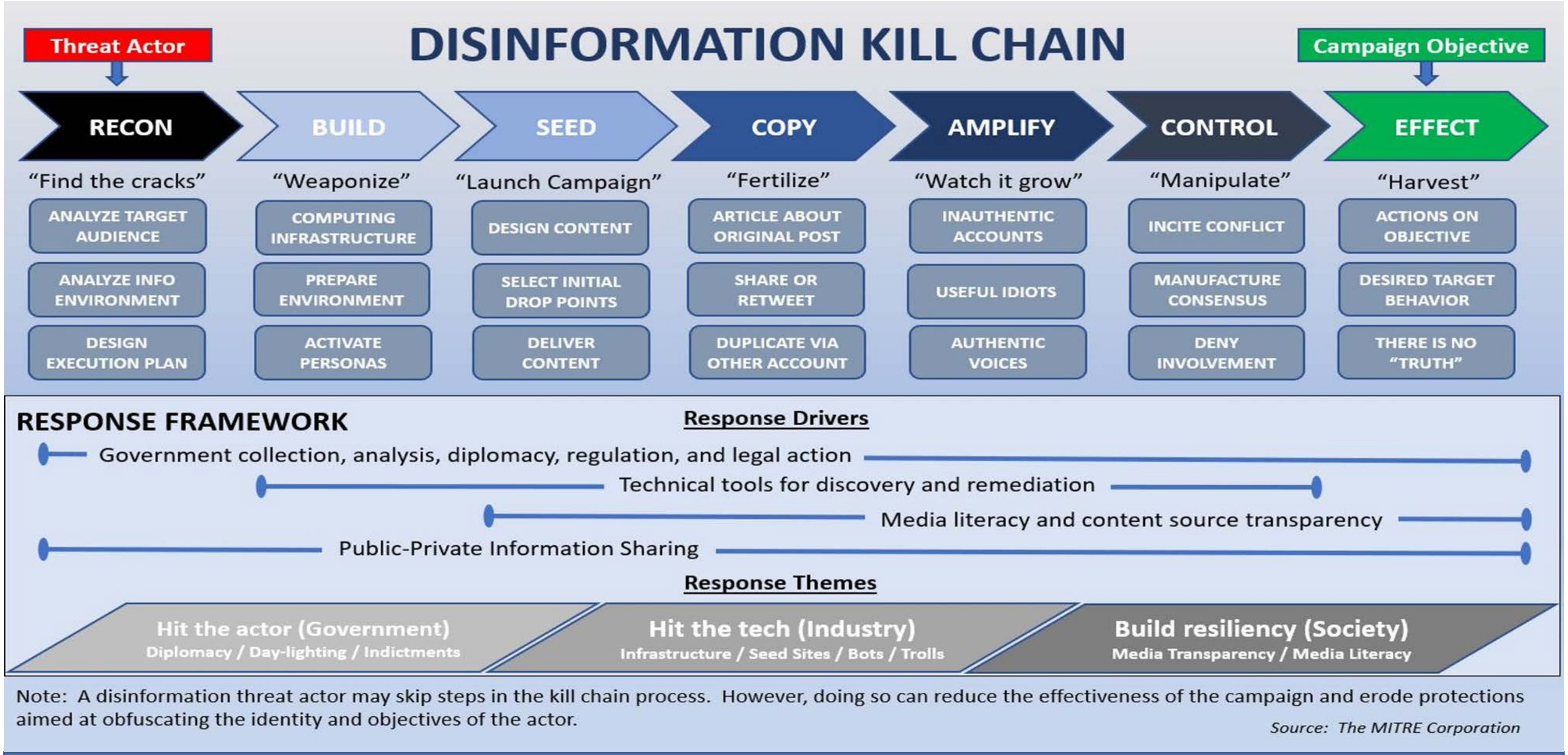
CONCLUSION

Since the events of the 2016 U.S. presidential election, the phenomenon of disinformation campaigns has received a great deal of attention, not just in the news media, but from government, academic, and commercial platforms determined to identify and understand it. While research efforts are plentiful, there is still much to learn about these campaigns and how best to defend against them. While it is not appropriate to dictate what media content Americans consume, we can, as researchers, suggest that opportunities for collaboration across interested sectors should continue to expand and to encourage public education to build resilience.

In a media environment where mere popularity, attention, and trending imbue truth and legitimacy, the internet can become a turbo-charged rumor mill with no editorial board. Disinformation can generate a lot of activity in a very short period of time, but whether this disinformation amounts to little more than noise in the system or represents a genuine threat is often not readily apparent. This paper emphasizes the importance of understanding targeted disinformation campaigns in the interest of hardening public defense against them. This includes understanding the threat actors who propagate these campaigns, how users are prone to them in a complex information environment and gaining the ability to identify these campaigns through their tell-tale signs.

Combatting disinformation campaigns by curtailing the free exchange of ideas could lead to a pyrrhic victory. Limits on free speech would further the objectives of threat actors seeking to weaken our democratic values. We must instead focus on building resilience, hitting the actor, and undermining their technical advantage. As these efforts mature, stakeholders can identify and counter campaigns "left of amplify," thus neutralizing the threat to democratic society and maintaining the integrity of our information environment.

Appendix: Disinformation Kill Chain



DISINFORMATION KILL CHAIN

Threat Actor

Campaign Objective

RECON – "Find the cracks"
- ANALYZE TARGET AUDIENCE
- ANALYZE INFO ENVIRONMENT
- DESIGN EXECUTION PLAN

BUILD – "Weaponize"
- COMPUTING INFRASTRUCTURE
- PREPARE ENVIRONMENT
- ACTIVATE PERSONAS

SEED – "Launch Campaign"
- DESIGN CONTENT
- SELECT INITIAL DROP POINTS
- DELIVER CONTENT

COPY – "Fertilize"
- ARTICLE ABOUT ORIGINAL POST
- SHARE OR RETWEET
- DUPLICATE VIA OTHER ACCOUNT

AMPLIFY – "Watch it grow"
- INAUTHENTIC ACCOUNTS
- USEFUL IDIOTS
- AUTHENTIC VOICES

CONTROL – "Manipulate"
- INCITE CONFLICT
- MANUFACTURE CONSENSUS
- DENY INVOLVEMENT

EFFECT – "Harvest"
- ACTIONS ON OBJECTIVE
- DESIRED TARGET BEHAVIOR
- THERE IS NO "TRUTH"

RESPONSE FRAMEWORK

Response Drivers

Government collection, analysis, diplomacy, regulation, and legal action

Technical tools for discovery and remediation

Media literacy and content source transparency

Public-Private Information Sharing

Response Themes

Hit the actor (Government)
Diplomacy / Day-lighting / Indictments

Hit the tech (Industry)
Infrastructure / Seed Sites / Bots / Trolls

Build resiliency (Society)
Media Transparency / Media Literacy

Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so can reduce the effectiveness of the campaign and erode protections aimed at obfuscating the identity and objectives of the actor.

Source: The MITRE Corporation

Information Types

Propaganda has a political connotation and is often connected to information produced by governments (the lines between advertising, publicity, and propaganda are often unclear).

Disinformation is manufactured information that is deliberately created or disseminated with the intent to cause harm.

Misinformation is false information shared without the intent to mislead.

Malinformation is genuine information, typically private or revealing, that may be distributed in a campaign to cause harm to a person's reputation to further the campaign s objective.

Inauthentic Information is *not* transparent in its origins and affiliation. The source of the information tries to mask its origin and identity.

Authentic Information is transparent in its origins and affiliation. The source of the information is unhidden.

Sources:

Claire Wardle, "Information Disorder: The Essential Glossary," *First Draft*, July 2018, https://firstdraftnews.org/wp content/uploads/2018/07/infoDisorder glossary.pdf?x19860
FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East," 21 August 2018, https://www.fireeye.com/blog/threat research/2018/08/suspected iranian influence operation.html