THE FUTURE OF DISINFORMATION OPERATIONS AND THE COMING WAR ON BRANDS

Adam Sohn
CEO, The Network Contagion Research Institute

Alex Goldenberg, Corresponding Author
Lead Intelligence Analyst, The Network Contagion Research Institute

Pamela Paresky, Author
Senior Scholar, The Network Contagion Research Institute;
Visiting Senior Research Associate, Stevanovich Institute on the Formation of Knowledge at the University of Chicago

Owen Early, Author
Analyst, The Network Contagion Research Institute

Lea Marchl, Author
Analyst, The Network Contagion Research Institute

Michael Gips, Author
Senior Advisor, Corporate Risk, The Network Contagion Research Institute

Joel Finkelstein, Author
Director, The Network Contagion Research Institute;
Fellow at the Miller Center for Community Protection and Resilience, Rutgers University

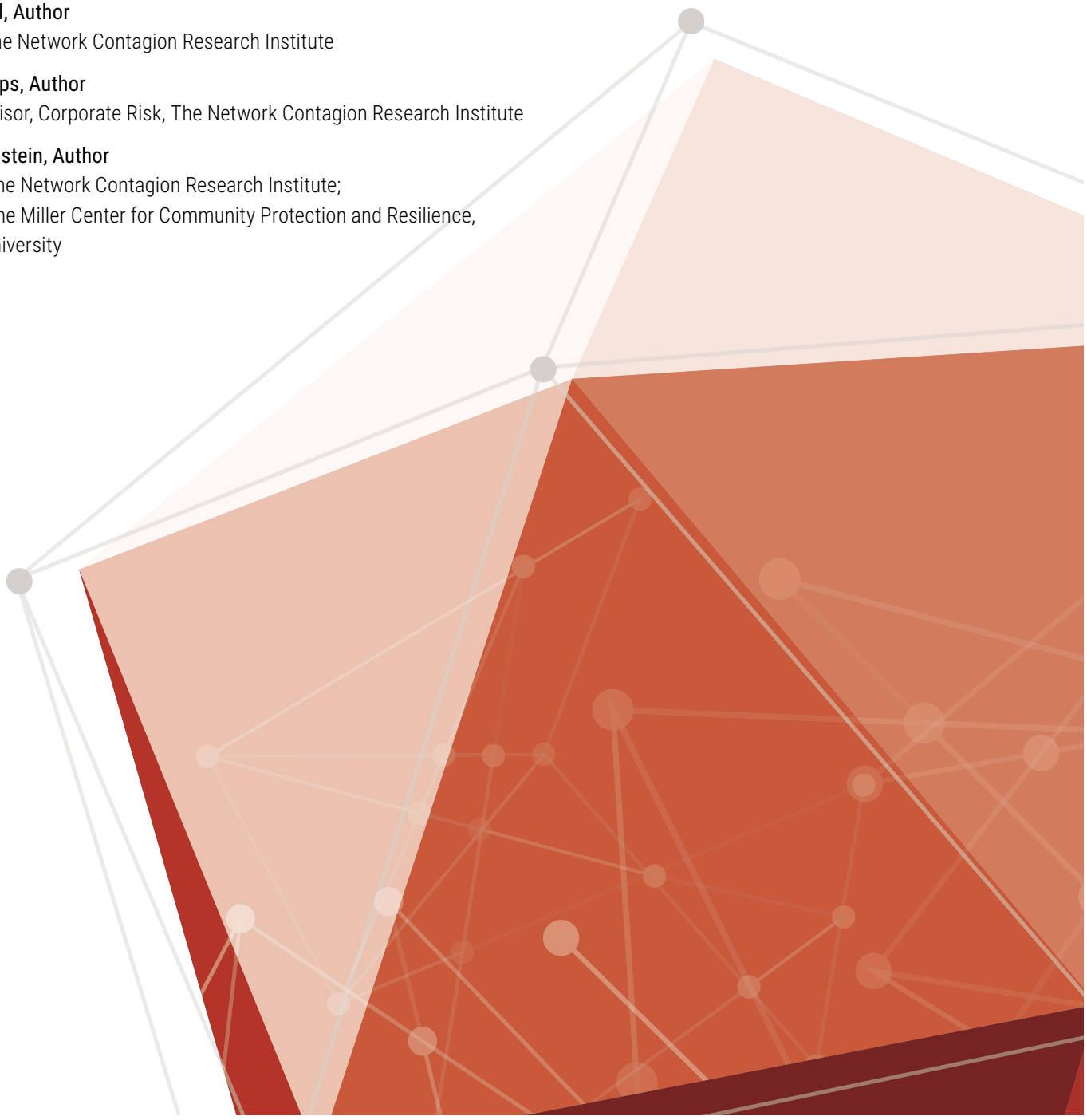
PRESENTED BY

RUTGERS
Miller Center for Community Protection and Resilience

RUTGERS
Center for Critical Intelligence Studies

POWERED BY

NETWORK CONTAGION
RESEARCH INSTITUTE



Disinformation has long been understood as a means of political warfare.[1] Now it is being used in ways that damage Western corporations and economies. The actors and methods employed to influence elections and spread conspiracy theories in an effort to polarize the United States electorate are now being leveraged for economic warfare. Additionally, an economic disinformation industry is emerging in which disinformation services are provided to domestic and foreign actors. As economic and political benefits of disinformation attacks accrue, this trend is expected to continue.

The brand disinformation ecosystem sits at the intersection between cyber risk and economics. It is massive, yet can be difficult to detect. Its real-world effect on companies can be devastating and long-lasting. For example Comet Ping Pong Pizza still suffers from picketing and protests; new videos proliferate on a daily basis spreading the Wayfair human trafficking conspiracy theory; and 5G cell towers continue to be targeted.[2] Within this ecosystem, a burgeoning industry of disinformation providers meets the growing demand for disinformation dissemination.

To explain the increase in private sector disinformation campaigns, a recent analysis[3] identified three broad areas of motivation driving actors to conduct them: financial gain, market disruption, and political activism. However, motives frequently overlap and we believe actors may be a more appropriate unit of analysis. Bad actors — ranging from state sponsored trolls to members of extremist groups to independent disinformation-service providers — can engage in all of these types of campaigns for reasons that range from greater notoriety to fee-for-service to ad revenue to secondary economic gain (e.g. product sales) to political and policy objectives.[4]

Thus far, the nature of the connection between state actors and disinformation in the economic sphere has been largely unexamined. For companies, an entirely new set of risks has appeared, creating a highly uncertain environment in which vulnerability to coordinated disinformation attacks now represents a serious threat to brand equity and even the physical safety of employees and customers.

State actors propagate disinformation using a variety of tactics as part of a set of economic strategies that promote their national interests. Disinformation is used by states not only as a form of political warfare to impact foreign elections and political processes, but as a pillar of economic warfare, with cyberattacks against businesses becoming an increasingly useful tactic to advance foreign policy objectives.

Campaigns and Conspiracies: 5G Conspiracy Theories; Inspiring Attacks on Infrastructure

Fifth-generation technology (5G) is the latest quantum leap for cellular networks, offering lower network latency and the ability to accommodate the simultaneous connections of phones, computers, and other "smart" devices.[5] According to the World Economic Forum, this capacity for "intelligent connectivity" is poised to add approximately $13.2 trillion of global economic value by 2035.[6] Closing the performance gap between current, hybrid 4G/5G networks and the touted "5G experience" requires network carriers to build out "standalone" infrastructure exclusively for 5G.[7] Some of these technological upgrades come in the form of short-range base stations ("small cell" towers) constructed at short intervals.[8]

The enormous cross-industry economic implications of 5G technology[9] have made its development and deployment a matter of intense competition among not only telecommunications firms, but countries concerned with its significance to national security. However, on social media, conspiracy theories about alleged negative health effects of 5G are rampant.[10] These conspiracy theories have been co-opted by Russia and China in an effort to discredit western 5G technology and promote their own. Both countries are engaged in massive social-media campaigns that employ a variety of state-owned and proxy media sources to disseminate disinformation.

The intentional fueling and amplification of conspiratorial narratives has already had dangerous, real-world consequences, including violent anti-5G protests and physical attacks on 5G small cell towers.[11] In 2020, dozens of attacks on cellular infrastructure were fueled by 5G conspiracy theories, and a San Diego man was arrested for arming himself against a feared Bill Gates 5G conspiracy theory.[12] This proliferation of 5G conspiracy theories, many of which are now intertwined with COVID-19 conspiracy theories, now threatens U.S. 5G infrastructure, associated companies, and their personnel. Last year, the Department of Homeland Security put the U.S. telecom industry on alert about related potential cell tower attacks and risks to telecommunications workers.[14]

Russian efforts to undermine confidence in the U.S. rollout of 5G technology were underway by 2019 and involved several conduits of disinformation, including Russian state-sponsored English-language news outlets, English-language reports from Russian state-sponsored "think-tanks," and a covert social-media campaign.

The principal benefits of Russian disinformation techniques are the ability to craft different — and even opposing — narratives to appeal to different target audiences, and the ability to take advantage of the "media multiplier effect," the strengthened ability to influence discourse by simultaneously deploying disinformation on multiple media platforms. As an earlier RAND analysis of Russian propaganda noted, using multiple channels of dissemination increases perceived message credibility.[15]

In 2019, in an effort to create distrust of U.S. 5G technology, the English-language affiliate of Russia's state-run media network, RT (Russia Today) America, began to traffic in alarmist stories that discussed 5G technology in terms of a "massive health experiment" that poses grave health risks. Meanwhile, Russia's domestic-facing media outlets framed the country's own procurement of 5G technology as critical for national economic development.[16] In other words, in addition to the dissemination of 5G conspiracy theories by non-state actors, Russia itself has been targeting American-led 5G infrastructure with anti-5G conspiracy theories that appear not to apply to Russian 5G technology. These conspiracy theories are disseminated by Russia Today, Global Research, the Internet Research Agency, and are amplified by Twitter trolls and others.[17]

In addition to cable and satellite broadcasts, RT America also used social media and online streaming to air stories about the alleged negative health impacts of 5G. Its videos had among the highest viewership of news outlets on YouTube, with over 4 million subscribers, and billions of views per year.

NCRI sought to quantify the scale and structure of the makeup of information operations and conspiracy for 5G. With assistance from partners, open source platform analysis, and NCRI's flagship platform, Pushshift, NCRI identified over 600,000 articles mentioning 5G that were published between January of 2019 and July of 2021, with roughly 70,000 from known sources of disinformation. Although the majority of articles mentioning 5G were from trusted sources (CNN, FOX Business, WSJ, etc.), the most cited articles mentioning 5G are from known Russian disinformation sources, including the entities, Global Research and RT, and non-state actors like Natural News and Children's Health Defense.

NCRI also analyzed over 17 million Twitter posts mentioning 5G between July of 2018 and July 2021.[18] Starting with the COVID-19 pandemic, tweets mentioning 5G have included terms like stop5g, 5gkills, soros, gates, cancer, coronavirus and others. These developments showcase the flexibility of movements enabled by disinformation against brands. In this case, the onset of COVID-19, an unexpected source of national disturbance in public health, bolstered an unrelated, existing reservoir of disinformation around a technological dystopia. In April and May of 2020, there were times when posts about 5G accompanied by these terms reached an average rate of 100 tweets per minute. Additionally, roughly 19,000 YouTube videos about 5G have accrued over 180 million views since January 1, 2019. More than half of these videos amplified 5G conspiracy theories.

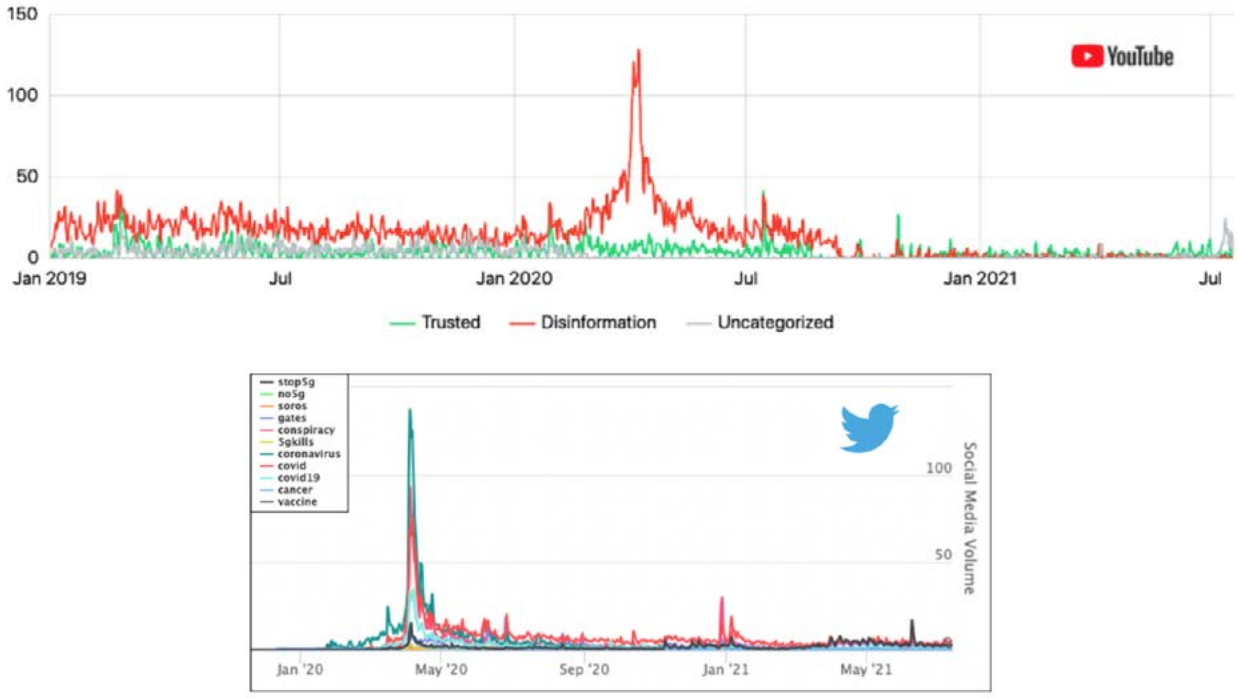


Figure 1. A partial time series analysis (see supplemental figure 1 for full graph) of multiple youtube videos (top) and hashtags tweeted per minute (bottom) mentioned with 5G. Conspiracy theories and disinformation around 5g appear to emerge in synchrony across platforms and show steep increases in response to the advent of the COVID-19 pandemic.

Figure 2. Major influencers such as Keri Hilson (Left) with over 4 million followers can unexpectedly amplify disinformation with implications to businesses while users innovate and experiment with new hashtags (Right) to provide a constant feed of inventive new conspiracy theory and material.

Anti-Vaccination Disinformation; Driving Vaccine Hesitancy

In an effort to degrade confidence in Western vaccines and promote Russia's Sputnik V vaccine, Russian intelligence agencies have been engaging in disinformation campaigns[19] that fuel a broader online anti-vaccine movement.[20] In addition to the standard tactic of disseminating negative coverage of Western vaccines, Russian marketing firms have directly approached social-media influencers in France, offering financial compensation for promoting fraudulent, allegedly "leaked" stories about Pfizer vaccine complications.[21]

Russia's vaccine disinformation campaigns also extend beyond the U.S. and Europe, and have focused on countries like Brazil, India, Indonesia, and Canada, which it sees as potential export markets for the Russain vaccine.[22] The Canadian website, Global Research, which generates over 7 million visits per year, frequently promotes the Sputnik V vaccines and denigrates American vaccines. According to the U.S. State Department, Global Research is directly linked to Kremlin proxies.

Another Russia-led disinformation campaign intended to damage the credibility of the Pfizer and Moderna vaccines in order to promote the Sputnik V vaccine is in the African market. In a Council on Foreign Relations blog post, members of Novetta, a disinformation tracking firm, revealed that in the Fall of 2020, well before vaccine makers had released any data to confirm vaccine effectiveness, public opinion of Sputnik V in Africa was suspiciously high. Novetta found that the Russian vaccine had the "second-highest rate of positive quotes (66 percent) in African media coverage" and the "the second-lowest negative perception (11 percent)." In the promotion of its vaccine, Russia has employed the time-tested propaganda method of publishing a high volume of positive news stories across several media platforms that rely on dubious information.[23]

To gauge the information landscape as it relates to American vaccines, NCRI has identified over 4 million articles since January of 2020 mentioning American pharmaceutical companies involved in COVID-19 vaccine production (Moderna, Johnson & Johnson, and Pfizer). More than half a million are from known disinformation sources, and the content generated from known disinformation outlets generates the most engagement. NCRI has also determined that sources connected to the Russian State (like Global Research and RT), and non-state actors (like Natural News and Children's Health Defense) have generated the most online articles on the topic, and those articles have been the most cited in other online articles.

To dissect how and when vaccine disinformation takes aim at specific brands in the social media sphere, NCRI collected over 8 million original tweets with the term "pfizer" from early 2009 to July 2021 and analyzed the prevalence of conspiracy terms in conjunction with mentions of the word "Pfizer." Interestingly, NCRI finds substantial increases in the use of these terms during the contested election of 2020. Here again, akin to 5g conspiracy, we see remarkable flexibility in conspiracy movements supported by disinformation. The onset of a contested election, which was an unexpected source of a national political crisis, bolstered an unrelated, existing reservoir of disinformation against Pfizer and other vaccine brands. Finally, a notable trend in the gathered Pfizer data is an increased frequency of 5G comments (Figure 3, bottom). This shows how movements supported by disinformation operations can jointly impact multiple brands through unexpected combinations. In fact, according to a recent Economist/YouGov poll, 1 in 5 Americans believe the U.S. government is using the Covid-19 vaccine to microchip the population. 5G is often a central theme in circulating vaccine microchip conspiracy theories.

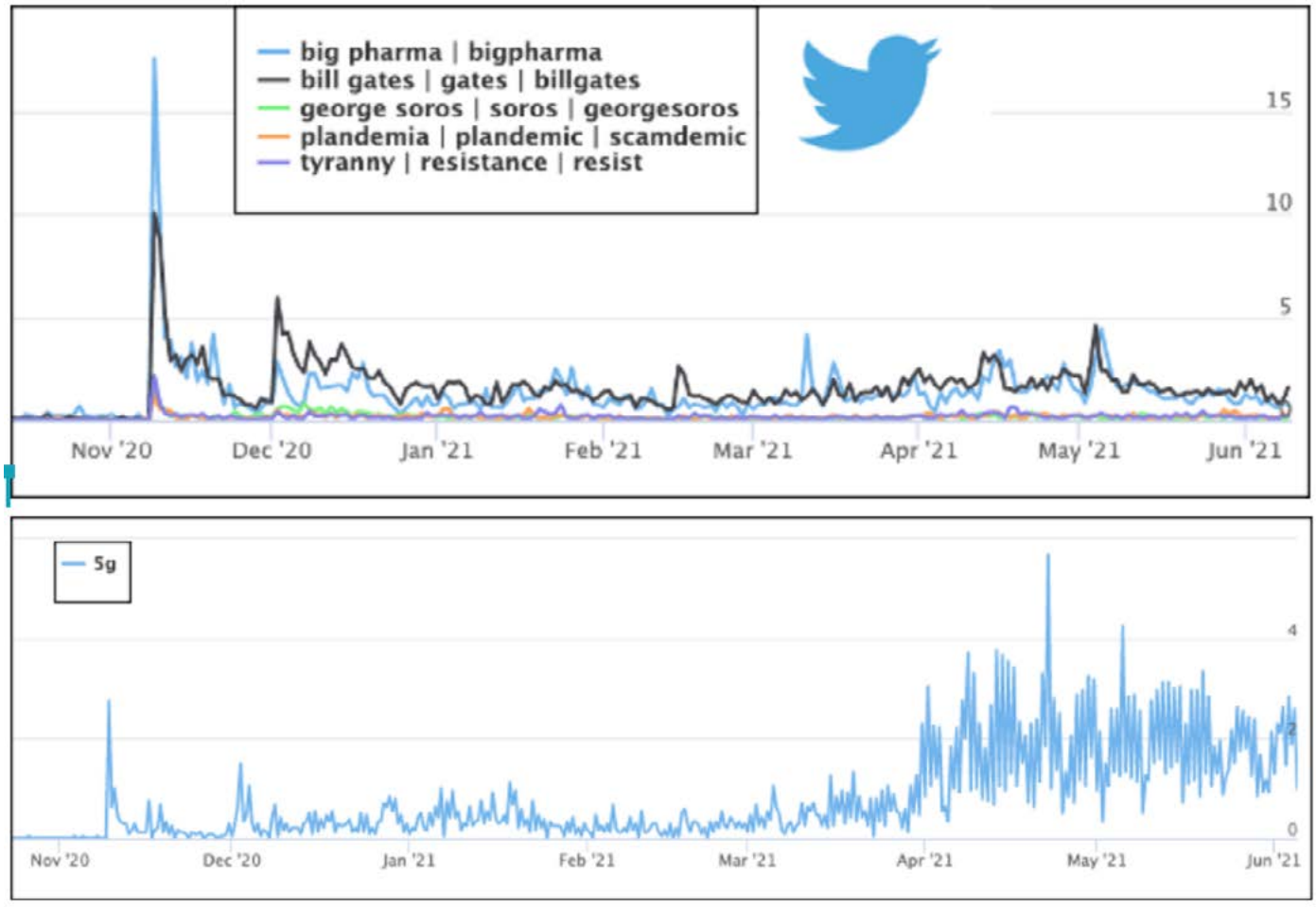


Figure 3 Top: An analysis of original tweets per minute (for full chart, see Supplemental Figure 2) with the term "pfizer" in combination with terms common to known covid disinformation narratives showed a substantial surge (up to 100 time per/minute) in putative conspiracy theory and disinformation. These surges occurred in tandem with ongoing election challenges in the United States and phase 3 clinical results for the vaccine. Bottom: 5g conspiracy chatter is increasing in connection to Pfizer and other vaccine brands on Twitter.

Disinformation in Retail and the Consumer Economy: State and Non-State actors

Both domestic and global consumer economies are at risk of targeted disinformation campaigns. In the United States, large corporations are routinely dragged into the "culture wars" as a result of false information originating from online conspiracy theory generators such as 4chan. In 2018, trolls on 4chan originated a fake coupon that purported to give free coffee to people of color in response to the widely reported incident involving two Black men in a Philadelphia Starbucks that resulted in a day-long closure of Starbucks nationwide for Racial-Bias education. The fake coupon was posted by an anonymous user on 4chan as a prank dubbed "Operation Mermaid." Likeminded users were encouraged to share it widely. Another user added a QR code that, when scanned, spelled out the n-word. The fake Starbucks coupon scandal was promoted and referenced by influential political commentators on other social media platforms, reaching millions of viewers and promoting outrage on Twitter.[24]

Figure 4. Trolls from 4chan and other fringe communities inflame racial tensions while attacking mainstream commercial brands, often with authentic-looking counterfeit material.

Other retail companies have also been affected by conspiracy theories originating from the conspiratorial fringes of the internet. On July 9, 2020, a post in the r/conspiracy subreddit alleged that furniture retailer Wayfair was at the center of a massive child trafficking ring. A day later, the company's name was trending on Twitter and the theory had spread across Facebook and TikTok.[25] As outlandish as the charge of child trafficking might seem, the Wayfair example demonstrates that disinformation attacks do not need even a kernel of truth to generate widespread negative publicity. A year later, dozens of new videos promoting the Wayfair theory are still posted on YouTube, illustrating the potential lasting effects of disinformation campaigns, irrespective of how swiftly conspiracy theories are debunked.

Globally, both state and non-state actors have targeted large corporations. Recent analysis from ProPublica and The New York Times revealed evidence of an influence operation designed to produce and spread thousands of videos of Chinese citizens denouncing foreign officials who are critical of the Chinese government's treatment of Uighurs in Xinjiang.[26] Videos that were banned in China appeared on a Communist Party news application (indicating they were intended for a Western audience) and spread on mainstream platforms like Twitter and Youtube in the U.S. and Europe. The campaign targeted foreign diplomats and retailers that had expressed concern about forced labor and other abuses in Xinjiang. Hundreds of videos flooded YouTube, TikTok, Twitter, and other highly subscribed mainstream platforms, accruing millions of views.

The Chinese Communist Party (CCP) also erased much of H&M's domestic internet presence across several platforms while amplifying narratives critical of H&M. In one YouTube video posted on CGTN, an international English-langauge news service operated by the CCP, someone toured the empty H&M flagship location in Beijing and recorded a handful of Chinese citizens expressing negative attitudes towards H&M, including, "the clothes are highly substitutable," and "I am very likely to boycott their goods." The video accrued over 270,000 views with thousands of comments denigrating Western retailers and supporting the Chinese government.[27] The significant pro-China sentiment and activity in the comment section is notable, as YouTube is inaccessible in Mainland China, and VPN usage is low.

Figure 5. Examples of comments left on CGTN YouTube video titled "Take a look at an H&M flagship store after Chinese people voice boycott." Notably, YouTube is inaccessible in Mainland China.

In response to the backlash, H&M published a statement reaffirming their long-term commitment to China, saying they hoped to regain the trust of customers in China.[28] H&M's attempt to reestablish goodwill in China triggered a subsequent Vietnamese boycott H&M campaign that exhibited signs of coordinated inauthentic online behavior. According to Japanese media, H&M, under pressure from authorities in China, posted a map on its website depicting disputed islands in the South China Sea as Chinese territory. [29]

To examine whether additional disinformation operations against H&M occurred in conjunction with this effort, NCRI analyzed 5.6 million comments from Twitter that contained "H&M" and analyzed activity. This analysis demonstrated that between April 2 and April 4, 2021, #BoycottHM was tweeted over 7,000 times (excluding retweets). Figure 6 shows that the use of the hashtag did not grow organically. Instead, it was retweeted at very high rates after being dormant, indicating coordinated inauthentic behavior. The most prolific account amplifying the #BoycottHM, was created the day the hashtag went viral. That account tweeted and retweeted posts that included the hashtag 550 times, likely in an effort to get #BoycottHM trending. A review of the nine next most prolific tweeters of the hashtag found that they retweeted each other's content and were only active during similar hashtag campaigns.

Figure 6. A time series analysis of #BoycottHM shows a spike in activity, all from self-identified Vietnamese accounts, which peaked at 75 times per minute.

These data cannot firmly establish whether this coordinated activity was conducted by Chinese disinformation agents posing as Vietnamese activists or Vietnamese activists with the wherewithal to engage in coordinated inauthentic activity. However, it illustrates that traditional brand and risk management strategies are insufficient to detect and manage new vulnerabilities in the emerging landscape of disinformation operations.

The Future of Disinformation Warfare

The scope and sophistication of disinformation attacks and the matrix of actors detailed above demonstrates a new security faultline that companies must anticipate as disinformation itself becomes a market commodity. State actors and the emerging disinformation-service industry may soon have automated disinformation capabilities, and natural-language processing may soon be used by adversarial actors to automate disinformation campaigns, potentially at scale.[30] This highlights the importance of corporations finding proactive mitigation strategies in the emerging brand disinformation ecosystem.

Disinformation attacks against businesses will only increase in frequency and scope, and as they do, new modes of disinformation will pose new and unique risks to brand equity, employee relations, general corporate culture, customer and employee safety, and consumer confidence. Without a comprehensive strategy for disinformation defense, these attacks will eventually monopolize the attention of corporate leadership, who will be required to manage unprecedented disinformation challenges.

Our analysis suggests that such a phase-change in the volume and sophistication of disinformation attacks is likely close at hand. These operations are already accelerated by artificial intelligence, deep fakes, progress in psychological profiling, advances in both the power and masking of influence operations, the burgeoning ecosystem of competing suppliers, and the combination of technology and financial resources of sovereign nations. Given these advances, along with the affordability and effectiveness of disinformation operations, disinformation attacks against corporations across numerous domains is likely to become commonplace.

To combat this, and avoid being caught off-guard, companies must now engage in focused capability-building around disinformation defense, and invest in resources for in-house analyses and forecasting. However, proficiency in the domain of disinformation defense is not yet widespread and may take years for businesses, or even consulting firms, to develop with any reasonable level of expertise.

In the face of these threats, many companies have thus begun to reach out to disinformation content experts to gain crucial insights quickly while developing internal analytic capabilities. Engaging topic experts in disinformation defense as well as investing in resources for in-house analyses and focused capability-building is imperative for companies to understand the web of actors and tactics in the world of brand and online disinformation.

Finally, unlike IP theft and cybersecurity, not only is the actuarial science of disinformation underdeveloped, it appears to be virtually non-existent. This means that an entirely new and dangerous category of risk exposure is looming for which American brands possess no protection. This fact cannot possibly be lost on the very disinformation agents assiduously seeking to undermine American brands. In light of these gaps, insurance providers would be well advised to innovate new instruments to capture and help companies mitigate disinformation risks using market based solutions.

FOOTNOTES

[1] The United States Senate's Select Committee On Intelligence report on "Russian Active Measures Campaigns And Interference in the 2016 U.S. Election" noted that "Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election."

[2] Jenny Gathright, "Conspiracy Theorists Protesting Comet Ping Pong Get Drowned Out By Lady Gaga," *DCist, WAMU 88.5*, January 19, 2021, Conspiracy Theorists Protest Outside Comet Ping Pong | DCist; EJ Dickson, "A Wayfair Child-Trafficking Conspiracy Theory Is Flourishing on TikTok, Despite It Being Completely False," *Rolling Stone*, July 14, 2020, Wayfair Trafficking Conspiracy Theory Spreading on TikTok - Rolling Stone; Sebastian Moss, "NYPD warns white supremacists and conspiracy theorists are targeting cell towers, critical infrastructure," *DatacenterDynamics*, March 18, 2021, NYPD warns white supremacists and conspiracy theorists are targeting cell towers, critical infrastructure - DCD (datacenterdynamics.com).

[3] "The disinformation age has arrived. Are you ready?" *PwC*, February 9, 2021, https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html; Mike Davis, "Three Types of Disinformation Campaigns that Target Corporations," *Nisos*, August 4, 2020, https://www.nisos.com/blog/disinformation-campaign-types/

[4] Joe Uchill, "Disinformation as service crosses borders with ease," *Axios*, October 3, 2019, https://www.axios.com/disinformation-misinformation-service-online-1da509b2-d535-4ab0-bd51-3ae2fc344e31.html; "Study: Google, Amazon ad revenue funds pandemic disinformation," DW, August 7, 2020, Study: Google, Amazon ad revenue funds pandemic disinformation | News | DW | 08.07.2020; Andrew Marantz, "Alex Jones's Bogus Coronavirus Cures," *The New Yorker*, March 30, 2020, Alex Jones's Bogus Coronavirus Cures | The New Yorker; "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements,"May 2018 report from the U.S. House of Representatives Permanent Select Committee on Intelligence, Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements | Permanent Select Committee on Intelligence (house.gov).

[5] Sascha Segan, "What is 5G," *PC Magazine,* February 25, 2021, https://www.pcmag.com/news/what-is-5g, https://www.cisco.com/c/en/us/solutions/what-is-5g.html

[6] "The Impact of 5G: Creating New Value across Industries and Society," white paper from the *World Economic Forum*, January 6, 2020, http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf, 9.

[7] Segan, "What is 5G," *PC Magazine.*

[8] James Meese, Jordan Frith, and Rowan Wilken, "COVID-19, 5G conspiracies and infrastructural futures," *Media International Australia* 177, no. 1, November, 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7506181/

[9]"The Impact of 5G: Creating New Value across Industries and Society,"16-18.

[10] "The Dangers of 5G to Children's Health," *Children's Health Defense*, February 13, 2019, https://childrenshealthdefense.org/news/the-dangers-of-5g-to-childrens-health/; "What You Need to Know About 5G Wireless and 'Small' Cells," *Environmental Health Trust*, https://ecfsapi.fcc.gov/file/10417078206082/5G_What%20You%20Need%20to%20Know_11.20.17%20(1).pdf.

[11] Elisabeth Braw, "The Imagined Threats of 5G Conspiracy Theorists Are Causing Real World Harm," *Foreign Policy*, June 29, 2020, https://foreignpolicy.com/2020/06/29/the-imagined-threats-of-5g-conspiracy-theorists-are-causing-real-world-harm/; Aaron Pressman, "Wireless industry fears 5G protest day could lead to damaged cell towers," Fortune, June 5, 2020, https://fortune.com/2020/06/05/wireless-industry-fears-5g-protest-day-could-lead-to-damaged-cell-towers/

[12] Justin Vallejo, "Coronavirus: Police seize guns and hold man over Bill Gates 5G Conspiracy Theory," *The Independent*, April, 28, 2020, Coronavirus: Police seize guns and hold man over Bill Gates 5G vaccine conspiracy | The Independent | The Independent.

[13] Meese, et al, "COVID-19, 5G conspiracies and infrastructural futures."

[14] Jon Brodkin, "The DHS Prepares for Attacks Fueled by 5G Conspiracy Theories," *Ars Technica/Wired*, May 24, 2020, https://www.wired.com/story/the-dhs-prepares-for-attacks-fueled-by-5g-conspiracy-theories/

[15] Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," *RAND* Corporation, 2016, https://www.rand.org/pubs/perspectives/PE198.html, 3-4.

[16] William J. Broad, "Your 5G Phone Won't Hurt You. But Russia Wants You to Think Otherwise," *The New York Times*, May 12, 2019, https://www.nytimes.com/2019/05/12/science/5g-phone-safety-health-russia.html; "Russia enters super-fast communication era with launch of first 5G zone in Moscow," RT America, August 8, 2019, Russia enters super-fast communication era with launch of first 5G zone in Moscow — RT Business News; "Russian telecom giant & China's Huawei launch 5G zones in Russian cities," RT America, August 30, 2019, Russian telecom giant & China's Huawei launch 5G zones in Russian cities — RT Business News.

[17] Broad, "Your 5G Phone Won't Hurt You. But Russia Wants You to Think Otherwise."

[18] 5g comments (below) only began mentioning most of the terms in the graph with any regularity in January 20.

[19] Disinformation about the Covid vaccines should not be confused with legitimate concerns about side effects such as myocarditis or questions about the potential for future health issues resulting from the use of mRNA vaccines.

[20] Michael R. Gordon and Dustin Volz, "Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, U.S. Officials Say," *The Wall Street Journal*, March 7, 2021, https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200

[21] Mark Krutov, et al, "Exclusive: Meet The Murky Russian Network Behind An Anti-Pfizer Disinformation Drive In Europe," *Radio Free Europe*, May 27, 2021, https://www.rferl.org/a/russia-pfizer-covid-disinformation-serebryanskaya-murky-vaccine-influencers/31277170.html

[22] "COVID-19 (Coronavirus) Disinformation Report - Volume 4.0," *Blackbird.ai*, November 19, 2020, https://www.blackbird.ai/reports/, 42.

[23] Beach Gray and Neil Edwards, "Russian Disinformation Popularizes Sputnik V Vaccine in Africa," *Council on Foreign Relations* blog post, December 10, 2020, https://www.cfr.org/blog/russian-disinformation-popularizes-sputnik-v-vaccine-africa

[24] Ben Popken and Brandy Zadrozny, "Trolls spread hateful fake starbucks coupon for 'people of color only,'" *NBC News*, April 19, 2018, https://www.nbcnews.com/business/business-news/trolls-spread-hateful-fake-starbucks-coupon-n867501

[25] Rachel E. Greenspan, "How the Wayfair Human Trafficking Conspiracy Grew Out of QAnon" *Insider*, July 13, 2020, Wayfair Human-Trafficking Conspiracy Theory Tied to QAnon (insider.com); "Fact check: No evidence linking Wayfair to human trafficking operation," Reuters, July 13, 2020, https://www.reuters.com/article/uk-factcheck-wayfair-human-trafficking/fact-check-no-evidence-linking-wayfair-to-human-trafficking-operation-idUSKCN24E2M2?fbclid=IwAR3WNOLt9DsNrMdwLO13mylatPo3CB-X3y7gsC1_H5GJ6yNC4Tj5kmgrFBE

[26] Jeff Kao, et al, "How China Spreads Its Propaganda Version of Life for Uyghurs," *ProPublica*, June 23, 2020, https://www.propublica.org/article/how-china-uses-youtube-and-twitter-to-spread-its-propaganda-version-of-life-for-uyghurs-in-xinjiang

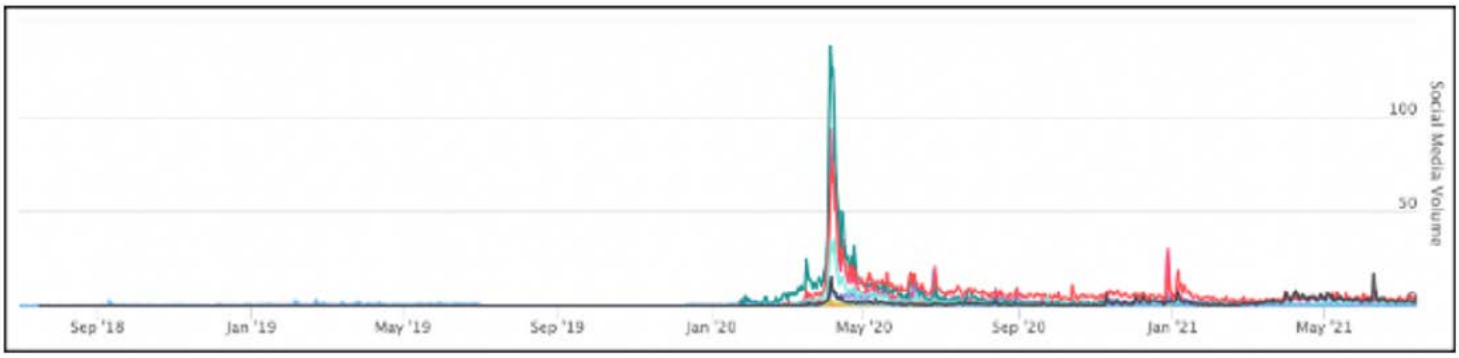
[27] "Take a look at an H&M flagship store after Chinese people voice boycott," YouTube video, CGTN News, March 26, 2021, 3:50, https://www.youtube.com/watch?v=E2UIg5wolnY.

[28] "Statement on H&M in China," *H&M Group*, March 31, 2021, https://hmgroup.com/news/statement_hm_china/

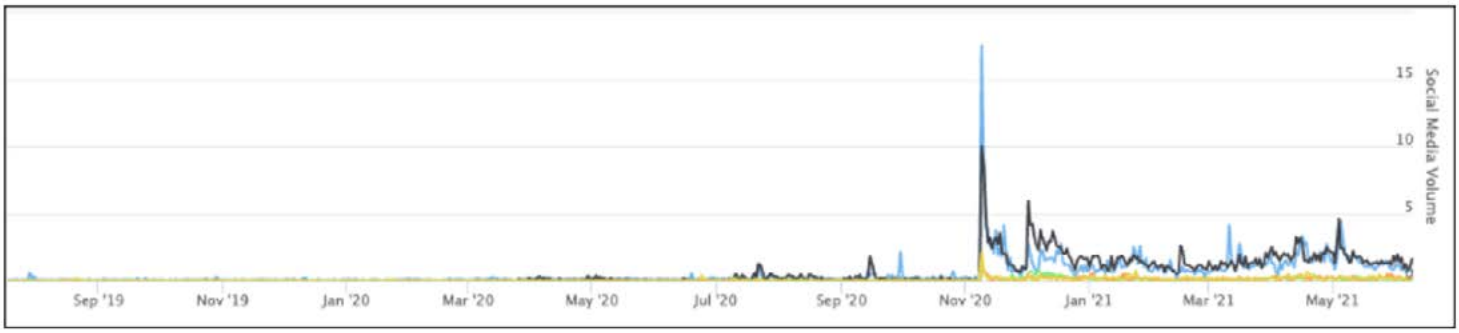
[29] Lien Hoang, "H&M faces Vietnam boycott over South China Sea map," *Nikkei Asia*, April 5, 2021, https://asia.nikkei.com/Politics/International-relations/H-M-faces-Vietnam-boycott-over-South-China-Sea-map

[30] Ben Buchanan et al, "Truth, Lies, and Automation: How Language Models Could Change Disinformation," *Center for Security and Emerging Technology*, May 2021, Truth, Lies, and Automation - Center for Security and Emerging Technology (georgetown.edu), 35-37.

SUPPLEMENTAL FIGURES



Supplemental Figure 1. The full timeline, starting fromJuly 2018, of Tweets featured in Figure 1.



Supplemental Figure 2. The full timeline, starting fromJuly 2019, of Tweets featured in Figure 3.

ACKNOWLEDGMENTS

storyzy

THE NETWORK CONTAGION RESEARCH INSTITUTE (NCRI) is a neutral and independent third party whose mission it is to track, expose, and combat misinformation, deception, manipulation, and hate across social media channels.

Acting as a public benefit corporation, NCRI is a not-for-profit organization that seeks to explore safe ways to audit, reveal challenges, devise solutions, and create transparency in partnerships with social media platforms, public safety organizations, and government agencies.