CSIS BRIEFS

Foreign Malign Influence Targeting U.S. and Allied Corporations

By Daniel Byman

MARCH 2025

THE ISSUE

U.S. corporations are regular targets of foreign governments seeking to undermine the United States. These hostile states have both commercial and strategic motives, and they use disinformation, malinformation, and artificial promotion to tarnish the reputations of U.S. companies. U.S. corporations and the U.S. government should take steps to mitigate this threat, including improving corporate counterintelligence, building networks of advocates for use in crisis situations, and sharing more information on the scope and scale of the problem.

Foreign governments have targeted U.S. and allied governments, the American people, and the citizens of allied countries with a wide range of disinformation, attempting to polarize politics and undermine confidence in government. Governments and populations, however, are not the only victims: Foreign governments also target U.S. corporations. Russia already often includes corporations in its attacks, and China is likely to do so more frequently as time goes on.

By attacking iconic U.S. companies, foreign governments can further divide Americans and undermine the credibility of the U.S. government. These attempts, however, have commercial effects in addition to strategic ones. Foreign malign influence campaigns have hurt U.S. companies' reputations, led to lost business opportunities, fostered dissatisfaction among workers, and created threats to the safety and well-being of mid-level and senior company members.

By attacking iconic U.S. companies, foreign governments can further divide Americans and undermine the credibility of the U.S. government.

To understand the threat of anti-corporate disinformation, this paper draws on interviews of security-focused individuals at a range of U.S. companies, interviews of disinformation experts, and media and academic sources. The interviews were conducted off the record, and a number of interviewees commented on other companies as well as their own. Almost certainly, these sources greatly underestimate the amount of anti-corporate disinformation; many of those interviewed made clear their companies had a hard time tracking the level and nature of disinformation being used against them. Identifying the ultimate source of disinformation is difficult, and many corporations are unaware of the origin of reports and the true ownership of various accounts speaking against them. U.S. government agencies and social media companies also pay far less attention to anti-corporate disinformation than they do anti-government or anti-society disinformation.

The paper first defines key terms and notes the prevalence of disinformation, malinformation, and artificial promotion. The second section discusses the motivations of foreign governments to engage in these tactics, with subsections focusing on the goals of Russia and China specifically, as well as their methods. The third section assesses commonalities of corporate foreign malign influence campaigns and their effects, and the final section concludes with recommendations to reduce the overall risk.

DEFINITIONS AND PREVALENCE

Foreign malign influence (FMI) can be defined as "subversive, undeclared, coercive, or criminal activities by foreign governments, non-state actors, or their proxies to affect another nation's popular or political attitudes, perceptions, or behaviors to advance their interests."[1] FMI often involves deliberately spreading *disinformation* (false information) or *malinformation* (truthful information that is presented or shared with the intent to harm, mislead, or manipulate). Unlike misinformation (false but unintentional) or disinformation (intentionally false), malinformation is based on fact but is used out of context or exaggerated to achieve malicious objectives.[2] A related and important concept is what several interviewees referred to as *artificial promotion*: when accurate but negative information is amplified to maintain its presence in the news cycle and visibility overall.

As the above definition suggests, FMI is usually thought of in the context of efforts by foreign states to discredit U.S. and allied governments. The long campaign of disinformation that the Soviet Union waged against the United States—which involved forgeries, spreading conspiracy theories, placing false articles in newspapers, and other efforts—is but one of many sets of historical examples. Moscow, for example, successfully spread the idea that the HIV virus originated in a U.S. biological weapons laboratory.[3]

Outside of the grand scale of the Cold War, information campaigns against companies, especially using malinformation, are nothing new. One official interviewed noted that companies regularly highlight the problems of their rivals, such as when a product functions poorly or there are malfeasance issues.[4] The official also noted that at times this is done through proxies, as the information is less credible when coming directly from a rival. In addition, customers sometimes put up false information about a company out of anger or spite, with an inaccurate (not just poor) review of a product or service. Hostile states are now joining in: Rafi Mendelsohn of Cyabra explains that "we're seeing a massive increase in the same techniques and methods that are used in elections—against governments and against societies—now being used against companies."[5]

Indeed, disinformation is now a service to be bought and sold. Disinformation-as-a-Service companies will write a short article for $50, author 10 comments to post for $100, assist with search engine optimization for $1,500, and otherwise spread falsehoods for a small fee.[6] Kekst CNS, a strategic communications firm, reports that 95 percent of FTSE 100 companies suffered from noncredible reporting, and 60 percent of companies say they suffered "substantial" or "some" harm from false reports of all sorts.[7] Fire on the Hill, another strategic communications firm, found that over half of the companies in their studies faced negative mis- and disinformation, and 10 percent claimed the damage was "substantial."[8] The spread of large language models and other forms of artificial intelligence are only making this easier and cheaper, greatly expanding its scale.

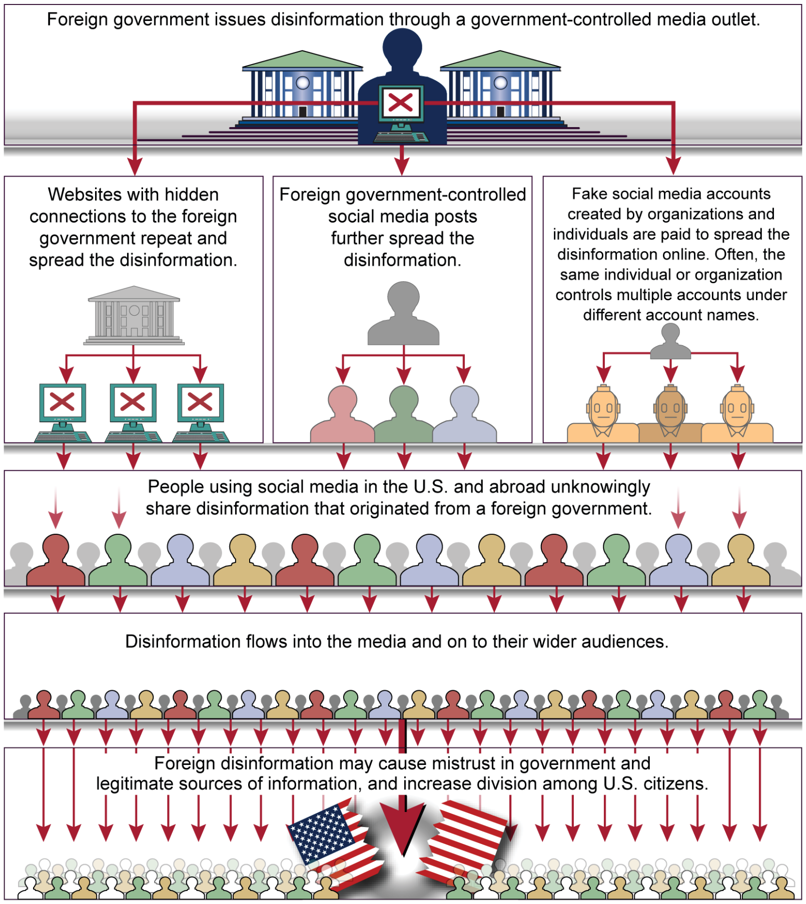
FOREIGN GOVERNMENT MOTIVATIONS AND APPROACHES

Foreign governments have many motivations for spreading disinformation and artificially promoting malinformation. Just as covert influence campaigns try to discredit the United States and other governments, foreign governments can shape U.S. and international public sentiment by casting aspersions on U.S. companies. Highlighting real and fake problems can foster mistrust in the United States, vindicating those who promote broader conspiracies about company products and policies. It can also reduce support for specific U.S. policies, such as arming Ukraine, by presenting companies involved in this effort as dishonest or having secret agendas. Finally, foreign governments may react to a CEO or other prominent corporate official's political or foreign policy stance.

Highlighting real and fake problems can foster mistrust in the United States, vindicating those who promote broader conspiracies about company products and policies.

Commercial goals are often at the top of the list.[9] When the reputations of U.S. and allied companies are hurt, foreign companies gain a competitive advantage. Beyond helping their own companies, foreign governments hostile to the United States seek to weaken U.S. economic power by hurting U.S. companies. The United States also has a range of iconic brands–Disney, Levi's, and Apple, among others–that in some ways represent the country, both at home and abroad. By tarnishing these brands, the U.S. "brand" is indirectly tarnished as well.

Figure 1: How Might Foreign Governments Quickly Spread Disinformation?


Foreign government issues disinformation through a government-controlled media outlet.
Websites with hidden connections to the foreign government repeat and spread the disinformation.
Foreign government-controlled social media posts further spread the disinformation.
Fake social media accounts created by organizations and individuals are paid to spread the disinformation online. Often, the same individual or organization controls multiple accounts under different account names.
People using social media in the U.S. and abroad unknowingly share disinformation that originated from a foreign government.
Disinformation flows into the media and on to their wider audiences.
Foreign disinformation may cause mistrust in government and legitimate sources of information, and increase division among U.S. citizens.

Source: "Foreign Disinformation: Defining and Detecting Threats," U.S. Government Accountability Office, September 26, 2024, https://www.gao.gov/assets/gao-24-107600.pdf.

RUSSIA

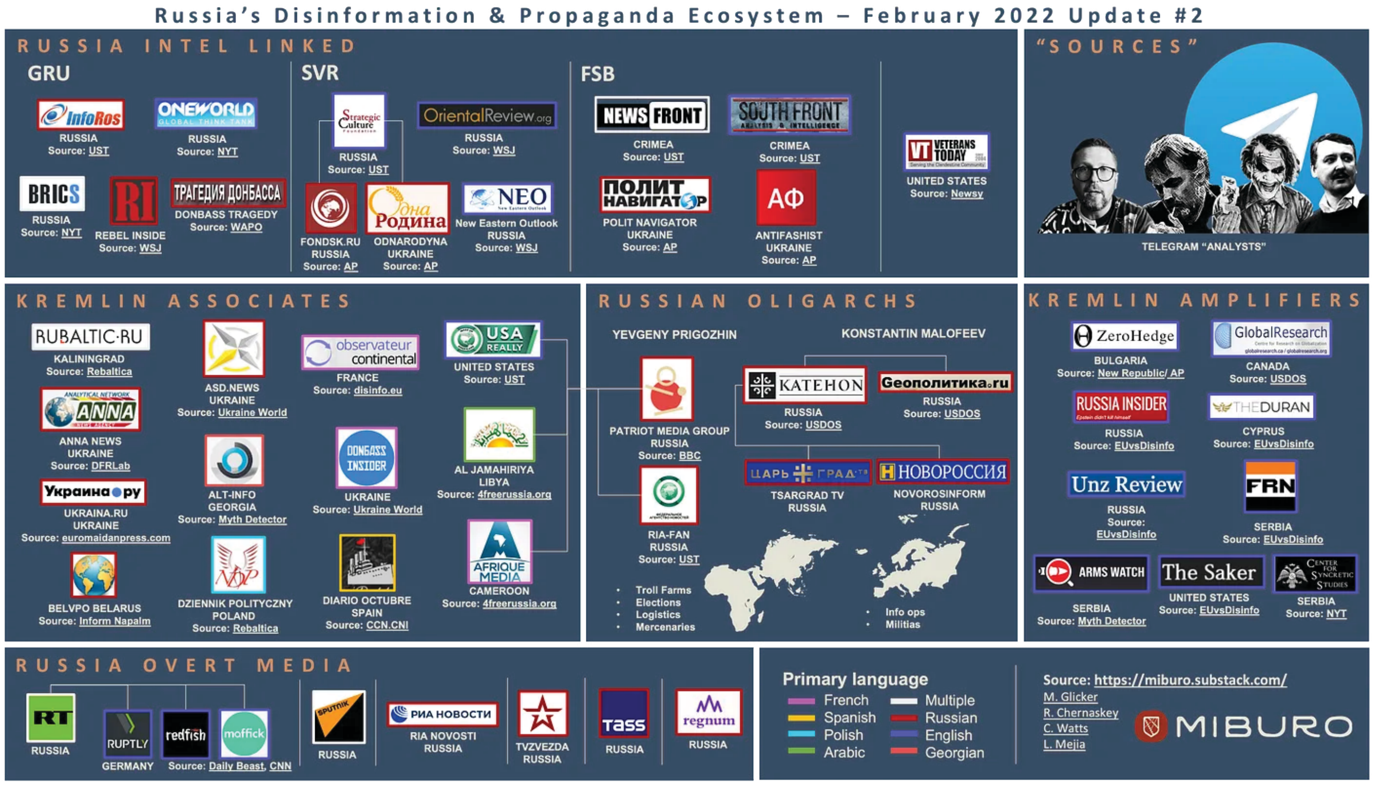
FMI fits into broader Russian hybrid warfare strategies. For example, Russian intelligence plotted to kill the CEO of Rheinmetall, Germany's largest arms manufacturing company, in retaliation for Germany's military support for Ukraine.[10] Moscow is also behind a broad campaign of sabotage throughout Europe, primarily targeting transportation and infrastructure targets, many of which are linked to European military support for Ukraine. Russian intelligence has also set "honey traps" (creating a sexual situation that can be used for blackmail) for both government and corporate leaders.[11]

Figure 1 illustrates how foreign governments use a range of sources, including websites they clandestinely control and fake social media accounts, to spread misinformation to large numbers of people.

As Figure 2 indicates, Moscow has a broad infrastructure to disseminate propaganda and disinformation. This includes not only the official government and media sources like RT, but also a wide range of actors supported by different intelligence services. The Russian Orthodox Church also plays a role, and Russian oligarchs use their reach to amplify Moscow's message, as do various Kremlin-associated outlets in Belarus, the United States, European countries, and occupied Ukraine, among other states. Russia also uses more specialized outlets to reach different audiences. RT America, for example, is targeted at the U.S. right, while "Watching the Hawks" is focused on the U.S. left. These various sources spread propaganda in many languages, and Moscow scatters the original sources among a wide range of supposed origin countries, such as India and Canada as well as Europe and the United States. Many articles, however, are originally published in English for wide distribution.

By design, these Russian sources interact with each other and build momentum for particular stories. Accounts on Facebook, X, and social media create rumors and chatter that official news media "cover." This coverage, in turn, is used to bolster social media campaigns by allowing them to link to official sources.

Figure 2: Russia’s Disinformation and Propaganda Ecosystem



Source: Clint Watts, “Russia’s Propaganda & Disinformation Ecosystem - 2022 Update & New Disclosures,” Selected Wisdom, February 15, 2022, https://clintwatts.substack.com/p/russias-propaganda-and-disinformation.

Conservative influencers in France, the United States, and other countries have repeated Russian propaganda lines, and Russia has reached out to them, although the degree of coordination is not clear.[12] Moscow often uses what disinformation scholar Chris Paul has labeled a “firehose of falsehood” approach, generating numerous false or exaggerated stories and then amplifying those that appear to be gaining traction.[13]

For Moscow, discrediting the U.S. government is a primary motivation. Russia has pursued this through multiple means, famously meddling with the 2016 election, among other activities.[14] For Russia, attacking a U.S. company is often a means to an end, not the ultimate target. Weakening the reputation of high-profile companies sows mistrust among the U.S. or allied publics in general. In 2023, Russia held a conference in Africa claiming that U.S. pharmaceutical companies were conducting biological testing in Africa under the guise of distributing vaccines—a way to use U.S. corporations as a way of discrediting the United States in general.[15]

Since 2022, Russian motivations have focused on discrediting those opposed to its war in Ukraine. As the Rheinmetall assassination attempt and many acts of sabotage in Europe indicate, Moscow is particularly focused on companies that play a role in bolstering Ukraine militarily.

CHINA

China’s motivations differ considerably from those of Russia, at least for now, and Beijing does not appear to have embraced FMI to the same degree that Russia has. While Russia’s motivation is more about destroying the global order and taking revenge on its enemies, Beijing’s anti-corporate FMI often follows a commercial rather than strategic logic. Much as in Russia, there is less of a public versus private delineation in China, with major companies expected to promote the government line while the government in turn advances the interests of major companies. Unlike Russia, however, China has many companies that are competitive in the global marketplace, and disinformation thus has more commercial advantages to Beijing than it does to Moscow.

China, for example, has indirectly promoted its vaccines and telecommunications by claiming that U.S. companies cannot be trusted. During the pandemic, China, along with Russia, cast doubt on Covid-19 mRNA vaccines, probably exacerbating hesitancy for this type of vaccine with the hope of increasing demand for the Sputnik and Sinovac vaccines.[16]

That said, there are also strategic grounds for China's disinformation campaigns, with the country seeking to discredit those who criticize its human rights abuses in Xinjiang, brutal labor practices, crackdown on democracy in Hong Kong, and other problems. For example, after the retailer H&M expressed concern about labor abuse in Xinjiang's textile industries, China coordinated a widespread propaganda campaign against H&M, including a nation-wide call to boycott the brand and a video campaign refuting allegations of labor abuse.[17] Beijing has targeted over 100 companies, including Walmart and the National Basketball Association.[18] In addition, a number of those interviewed for this report believed that as tension heats up over Taiwan, strategic motivations will soon follow: "Ukraine now, but Taiwan soon," is how one official put it.[19]

In contrast to Moscow's "firehose of falsehood," Beijing's approach emphasizes narrative consistency. It cares more about presenting a coordinated message, with its various trolls, influencers, and fake social media accounts echoing the messages put forward by state media rather than pursuing their own lines of attack.

COMMON FMI THEMES

Although the specifics vary by country and situation, corporations targeted by FMI have observed several common approaches. One is simply to try to flood the internet with tweets and other content generated by bots to create one-sided discourse. After Houston Rockets general manager Daryl Morey tweeted in support of Hong Kong, for example, the Chinese government unleashed a social media campaign that pretended to represent the views of outraged Chinese citizens.[20] A more subtle approach is backhanded good news. A campaign probably originating with Russia sought to tarnish Boeing, for instance, noting via social media: "Despite experiencing leaks and thruster failures, astronauts . . . remain confident in Boeing's Starliner."

Another approach is to push business-linked conspiracy theories that sow division. RT, for example, claimed that an investment firm shorted Trump stocks ahead of the attempted assassination attempt on him in July, while other propaganda portrays U.S. Ukraine war backing as a business opportunity for U.S. arms manufacturers. Similarly, Russia amplified the 2017 dispute over NFL players taking a knee during the national anthem, promoting Twitter hashtags like #boycottNFL to damage the NFL brand and hurt overall sales.[21]

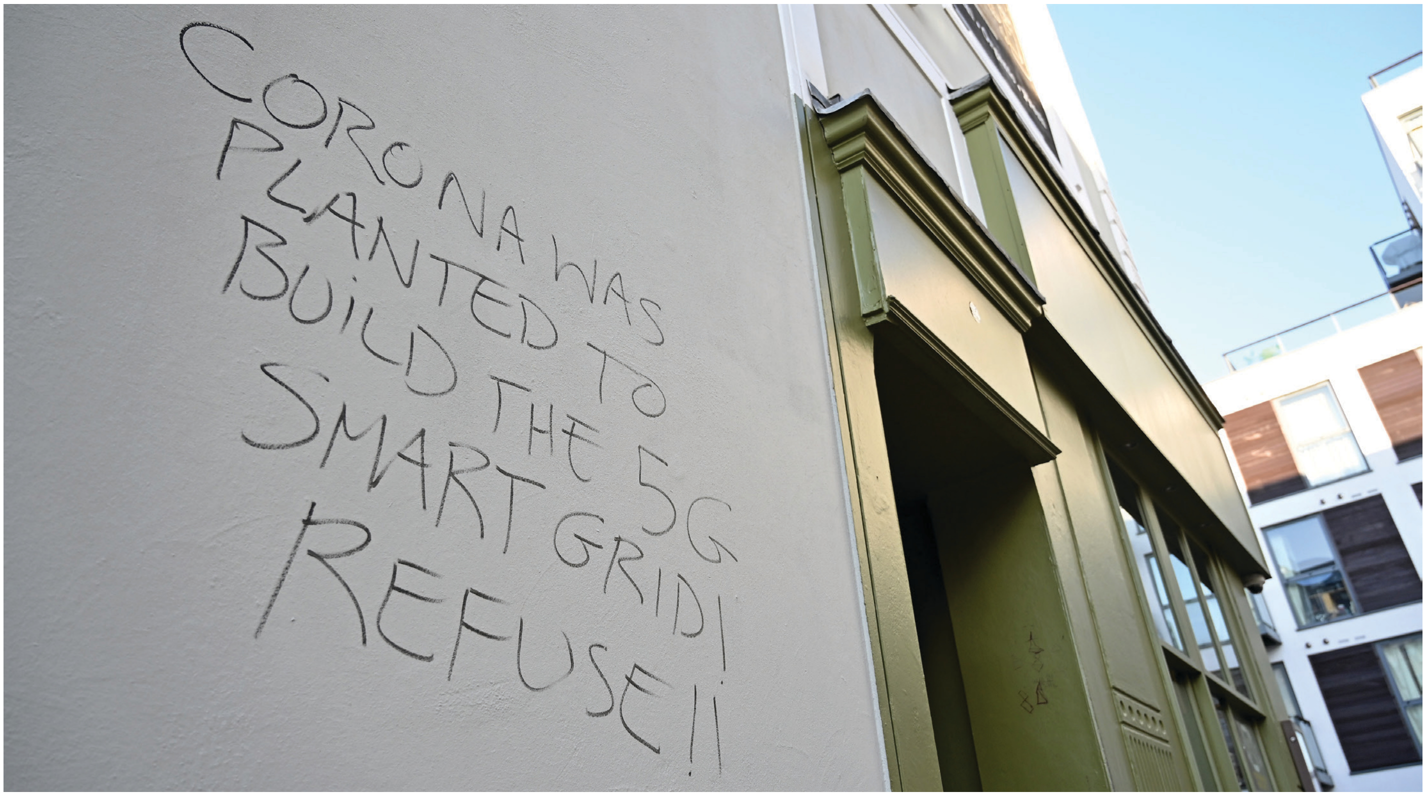
Artificially amplifying actual bad news for a company is also common. Problems with products—such as Boeing's well-publicized problems with the 737 Max—understandably command media attention, but foreign support can keep social media mentions of the problems artificially high. Russia-associated accounts began to push outlandish claims that Boeing had hired a hitman as well as broader narratives that Boeing planes were unsafe. Officials at several companies noted that bad news stayed prominent longer than expected based solely on the news value of the stories.

To increase divisions, FMI will often latch onto existing points of tension. For example, a Kekst CNC report found that falsehoods about business adherence to climate targets rose around COP27.[22] During the Israel-Hamas War, Russian FMI highlighted ties to Israel to discredit U.S. arms manufacturers. Similarly, claims that a company hired less-qualified engineers due to DEI requirements were used to explain a company's problems and thus magnify the attention being brought to them. Before the 2022 midterm elections, Russian disinformation platforms like the Red Spring Information Agency and the Centre for Research on Globalization, along with various Russian-linked social media accounts, spread disinformation about Dominion Voting Systems (which had been at the center of false reports in the 2020 election), seeking to decrease confidence in U.S. elections.[23]

IMPACT OF FMI ON CORPORATIONS

Anti-corporate FMI has several potential negative effects. Foreign support can contribute to a higher volume of negative stories about a company and a longer life for both real and fake negative news. When a company's reputation is being questioned, it increases market uncertainty and can decrease trade volume. For example, in a piece of disinformation of uncertain origin, a forged Department of Defense memo asking for a review of Broadcom's acquisition of CA Technologies led Broadcom's stock to drop sharply.[24] One official of a leading U.S. company noted that due to FMI, minor, but real, problems with their product "that would have been ignored after 24-48 hours in the news" persisted for weeks due to foreign amplification.[25]

Companies can also lose business opportunities. Governments may hesitate to work with a company whose reputation is being questioned, leading to lost or delayed contracts. Rival companies, both foreign and domestic, may supplant the company in question if its products or



Graffiti linking multiple conspiracy theories that discredit telecommunications companies.

Photo: Justin Tallis/Getty Images

overall reputation are tarnished. One official interviewed believed that their company lost several important sales as a result of FMI.[26] The brand as a whole may be tarnished, decreasing overall consumption of the product.

Physical threats and other workforce risks are also possible. As reputation declines, it is harder to attract top workers. There may also be a physical threat to facilities, with violent demonstrations a possibility. One official recounted that FMI contributed to hostile pro-Palestine demonstrations outside corporate headquarters, as their company provided services to the Israeli military.[27] Mid-level people, not just senior CEOs, have been "doxxed" or otherwise had their identities revealed in FMI-linked campaigns, leading to cyber mobs and at times in-person threats.

During the pandemic, RT spread disinformation about the negative health effects of exposure to 5G, pushing this on YouTube and other social media. Some of the most-cited sources on 5G came from Russian propaganda outlets.[28] This disinformation led to attacks against the communications infrastructure, with dozens of arson attacks in the United Kingdom and the Netherlands, as well as threats to and harassment of Dutch and Swedish engineers and industry representatives.[29]

IMPLICATIONS AND RECOMMENDATIONS FOR COUNTERING ANTI-CORPORATE FMI

FMI is difficult to counter, regardless of whether it is targeting people, societies, or corporations. False negative news travels quicker than positive news, and fact-checking and other corrections often make little impact once a story is told.[30] There are a wide range of influencers, social media accounts, and other sources to monitor, including many obscure ones that are not typically followed by even large companies. Following anti-corporate FMI is not a government priority, leaving companies largely on their own.

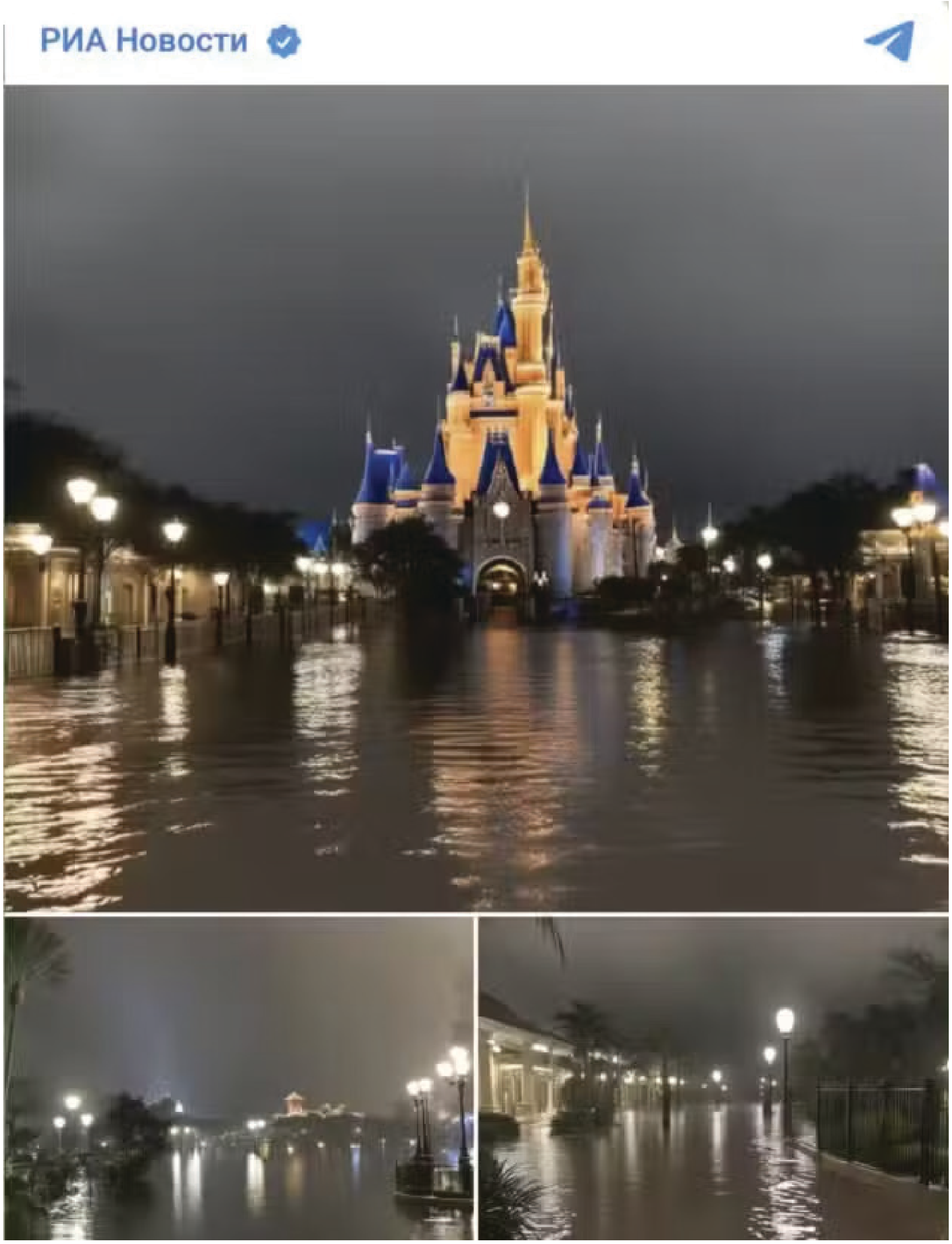
This problem is likely to get worse in the years to come. The Trump administration has downplayed the threat of FMI in general—especially from Russia—and it appears that offices in the Office of the Director of National Intelligence, State Department, and other entities that are monitoring it are likely to be slashed. Social media companies, for their parts, are also investing less in content moderation and other efforts to police their own platforms.

RIA Novosti

Multiple Russian state-owned news agencies

"Hurricane Milton flooded Disney World in Florida. People are walking knee-deep in water."

Source: Business FM, Oct. 10, 2024



AI-generated fake images of a flooded Disney World circulated on Russian media accounts in October 2024.

Photo: RIA Novosti (web screenshot)/VOA News

Advancements in deepfake generation are likely to further worsen this problem, as they enable governments and private individuals to rapidly generate high-quality disinformation and disseminate it quickly. As observed in a prescient 2018 study:

> Deep-fake videos could show a rival company's chief executive engaged in any manner of disreputable behavior, from purchasing illegal drugs to hiring underage prostitutes to uttering racial epithets to bribing government officials. Deep fakes could be released just in time to interfere with merger discussions or bids for government contracts . . . mundane business opportunities could be thwarted even if the videos are ultimately exposed as fakes.[31]

In a recent example, AI was used to generate fake images of Disney underwater after Hurricane Milton in October 2024, and then this was publicized on Russian media and social media accounts.[32]

What measures, then, can be taken to reduce the impact of FMI? While it may not always matter, attribution can be helpful. Knowing who is behind a campaign can shed light on what is driving the disinformation and malinformation, and highlighting this may help counter them. Similarly, "pre-bunking" may be helpful: alerting media and independent influencers in the early stages of an FMI campaign, letting them know it may be underway before it becomes a significant problem. However, companies may have business reasons to want to avoid alienating governments, even hostile ones.

Corporations that seek to reduce the impact of FMI should consider several steps. One is to build a broad network of advocates on social media that can advance a more positive narrative. This step can be outsourced to specialized public relations companies, as it requires an investment of time and resources to convince individuals—the more independent, the better—of the value of the corporation's products and services and the honesty of its corporate communications. In a crisis, this will pay off, enabling broader support in the face of lies and uncertainty.

Companies can also coordinate among themselves, sharing common techniques that Russia and other countries use as well as possible mitigation measures. As one official noted, "security is not a competitive sport." Some companies coordinate at least informally, while others see little need as they are unaware of the potential risk.

Corporate leaders also need to learn about counterintelligence, which is not natural for them—one security official described a "blank look" whenever they brought up FMI issues.[33] Counterintelligence briefings should be expanded, ideally in combination with government briefings. Corporate leaders must understand how their words can be manipulated or taken out of context, exercise careful information security, and otherwise recognize that foreign governments see them as legitimate targets. Removing personally identifiable information (PII) of even mid-level corporate officials may also be necessary if the risk of doxxing or real-world violence is high. This will be especially important if China steps up its efforts, as it has many companies that seek commercial advantage over their U.S. rivals.

Corporate leaders also need to learn about counterintelligence.

The U.S. government can play a helpful role in reducing the risk of FMI. One simple step is to issue reports on the scope of the problem and indicators when a campaign is underway. The government could also require more reporting from company officials on FMI, comparable to what it does on cyber incidents; better sharing of information would increase understanding of the scope and scale of the problem and its likely perpetrators. Ideally, governments would coordinate with company officials, warning them as campaigns are building and passing on information that could be publicly shared to inform the media and provide accurate information to the public. Governments can also avoid ambiguous sanctions and other pressure that ostensibly give companies wiggle room on enforcement, and, in so doing, put them in the crosshairs of foreign governments that want to influence corporate decisions. Finally, public indictments can be useful, giving companies a stronger legal basis on which to act and highlighting bad actors.

The U.S. government should also consider offensive measures, both against the particular entities promulgating disinformation and malinformation and, more directly, against the foreign governments themselves. This may involve working with allies to boycott Chinese or other foreign companies if they are linked to FMI campaigns. It also may involve offensive cyber operations, information campaigns to highlight corruption and human rights abuses among adversaries, and other means to impose real costs on Russia and other governments that use these techniques. ■

***Daniel Byman** is the director of the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

The author would like to thank Jamie Landy for his help with the research; Iselin Brady and Skyeler Jackson for their assistance with editing and finding sources; Seth Jones for his comments on an earlier version of this paper; and Phillip Meylan, Hunter Hallman, and Kelsey Hartman for their assistance with the publication process.

CSIS BRIEFS are produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

Cover Photo: Skórzewiak/Adobe Stock

ENDNOTES

1. "The Foreign Malign Influence Center," Office of the Director of National Intelligence, https://www.dni.gov/index.php/fmic.
2. "Misinformation, Disinformation & Malinformation: A Guide," Princeton Public Library, https://princetonlibrary.org/guides/misinformation-disinformation-malinformation-a-guide/.
3. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); and Aaron F. Brantly, "A Brief History of Fake," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (London: Routledge, 2020), https://www.taylorfrancis.com/chapters/edit/10.4324/9780429470509-3/brief-history-fake-aaron-brantly.
4. Virtual interview with U.S. corporate officials, August 2024.
5. Rebecca Pardon, "The Dangers of Disinformation for Companies," *Communicate Magazine*, December 18, 2023, https://www.communicatemagazine.com/news/2023/the-dangers-of-disinformation-for-companies/.
6. "Disinformation Attacks Have Arrived in the Corporate Sector. Are You Ready?," PricewaterhouseCoopers, February 9, 2021, https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html.
7. Elisabeth Braw, "Corporations Are Juicy Targets for Foreign Disinformation," *Foreign Policy*, August 15, 2024, https://foreignpolicy.com/2023/12/05/corporations-foreign-disinformation/.
8. Chris O'Toole, "Fire on the Hill Puts Mis- and Disinformation on the Corporate Agenda in Washington DC," Fire on the Hill, May 7, 2024, https://fireoth.com/en-us/2024/06/24/fire-on-the-hill-puts-mis-and-disinformation-on-the-corporate-agenda-in-washington-dc-us/.
9. Braw, "Corporations Are Juicy Targets."
10. Paul Kirby, "German Shock at Reported Russian Assassination Plot," BBC, July 12, 2024, https://www.bbc.com/news/articles/c1wej84e9l7o.
11. Duncan Gardham, "Russian Spies in Love Triangle Were to Be Used in 'Honeytrap' Operation across Europe, Court Hears," Sky News, November 28, 2024, https://news.sky.com/story/russian-spies-in-love-triangle-were-to-be-used-in-honeytrap-operation-across-europe-court-hears-13262616.
12. Pamela Paresky et al., *The Future of Disinformation Operations and the Coming War on Brands* (Princeton, NJ: Network Contagion Research Institute, July 2021), https://networkcontagion.us/wp-content/uploads/NCRI-%E2%80%93-The-Future-of-Disinformation.pdf.
13. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND Corporation, July 11, 2016), https://www.rand.org/pubs/perspectives/PE198.html.
14. Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* (Washington, DC: U.S. Department of Justice, March 2019).
15. Michael Gordon et al., "Russian Intelligence Is Pushing False Claims of U.S. Biological Testing in Africa, U.S. Says," *Wall Street Journal*, February 8, 2024, https://www.wsj.com/world/africa/russian-intelligence-is-pushing-false-claims-of-u-s-biological-testing-in-africa-u-s-says-ea817592.
16. Ben Dubow, Edward Lucas, and Jake Morris, *Jabbed in the Back: Mapping Russian and Chinese Information Operations During the COVID-19 Pandemic* (Washington, DC: CEPA, December 2021), https://cepa.org/comprehensive-reports/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-the-covid-19-pandemic/; and Robin Emmott, "Russia, China Sow Disinformation to Undermine Trust in Western Vaccines," Reuters, April 28, 2021, https://www.reuters.com/world/china/russia-china-sow-disinformation-undermine-trust-western-vaccines-eu-report-says-2021-04-28/.
17. Jeff Krolik et al., "How China Spreads Its Propaganda Version of Life for Uyghurs," ProPublica, June 23, 2021, https://www.propublica.org/article/how-china-uses-youtube-and-twitter-to-spread-its-propaganda-version-of-life-for-uyghurs-in-xinjiang.
18. Victor Cha, "Examining China's Coercive Economic Tactics," CSIS on the Hill, May 10, 2023, https://www.csis.org/analysis/examining-chinas-coercive-economic-tactics.
19. Virtual interview with corporate officials, September 2024.
20. "An NBA Controversy Sparks Social-Media Manipulation," *The Economist*, October 30, 2019, https://www.economist.com/graphic-detail/2019/10/30/an-nba-controversy-sparks-social-media-manipulation.
21. Phil Helsel, "Russian Trolls Using NFL Protests to Sow Discord Online, Republican Senator Says," NBC News, September 27, 2017, https://www.nbcnews.com/news/us-news/russian-trolls-using-nfl-protests-sow-discord-online-republican-senator-n805296.
22. Braw, "Corporations Are Juicy Targets."
23. "Hoax in the Machine: Disinformation against Voting Systems Manufacturers and Technologies in the 2022 US Midterm Elections," Recorded Future, November 7, 2022, https://www.recordedfuture.com/blog/hoax-in-the-machine-disinformation-against-voting-systems-in-the-2022-us-midterm-elections.
24. Tom Jowitt, "Broadcom Hits Out At 'Fake' Pentagon Memo Of CA Acquisition," Silicon, October 11, 2018, https://www.silicon.co.uk/e-enterprise/merger-acquisition/broadcom-fake-pentagon-memo-ca-237791; and Aaron Pressman, "How Broadcom Stock Was Hit by a Fake National Security Scare," Yahoo!finance, October 10, 2018, https://finance.yahoo.com/news/broadcom-stock-hit-fake-national-180038217.html?guccounter=1.
25. Virtual interview with U.S. corporate officials, August 2024.
26. Ibid.
27. Ibid.
28. Paresky et al., *The Future of Disinformation Operations*, 3.
29. Elisabeth Braw, "5G Conspiracy Theorists and Anti-Vaxxers Are

Using Online Propaganda to Fuel 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/; and William J. 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/2019/05/12/science/5g-phone-safety-health-russia.html.

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

31. Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *SSRN Electronic Journal* (2018): 1775, https://doi.org/10.2139/ssrn.3213954.

32. "Russian State Media Uses AI-Generated Images of Florida's Disney World Flooded by Milton," Voice of America, October 11, 2024, https://www.voanews.com/a/russian-state-media-uses-ai-generated-images-of-florida-s-disney-world-flooded-by-milton/7819396.html.

33. Interview with U.S. corporate official, October 2024.