Reputation Warfare

Weaponized Disinformation, Corporations, and Critical Infrastructure

Table of Contents.

IF Insight Forward

Introduction

Weaponizing information, including dis- and misinformation, is nothing new to the political and geopolitical realms. Rumors that the British were using beef and pork fat in the grease for cartridges was the proximate cause of the Indian Rebellion of 1857. Misinformation about the cause of the explosion on the *Maine* led America to declare war against Spain in 1898. During the Cold War, the Soviet Union spread malicious conspiracies about the U.S., such as America inventing the AIDS virus. The U.S. also used information operations to convince people of the evil of communism and the Soviet Union. What has changed in the early 21st century is that weaponized information is now working against corporations as well. In fact, corporations have been the direct target of disinformation that has impacted both their market share and security. However, weaponized disinformation is not just about falsehoods; the political polarization of the Western polity, particularly in the United States, has increased the risks to corporations rightly or wrongly associated with particular ideologies or policies.

Disinformation is a core component of what is termed hybrid threats today because it amplifies the complexity and effectiveness of multifaceted attacks, which blend conventional and unconventional strategies to destabilize targets without (necessarily) engaging in outright warfare.[1] To start, disinformation campaigns aim to erode trust in institutions, by spreading false narratives about election integrity, public health measures, or corporate actions, threat actors can make populations more vulnerable to further manipulation. Scholars have already noted that "a single carefully crafted and perfectly timed piece of (dis)information can now potentially make or break elections, governments, economies, and infrastructures, thus granting tremendous leverage to those who know how to weaponize and manipulate these critical systems."[2]

This can be especially harmful as disinformation can undermine responses to actual crises. This tactic overwhelms emergency response and leaves populations confused or distrustful of authorities. Importantly, disinformation can be used in conjunction with cyberattacks, economic coercion, or military actions to amplify the perceived impact. For example, after a cyberattack disinformation can exaggerate the scale of the damage, blame specific groups or governments, or sow panic among the public, intensifying the effect of the attack.[3] Disinformation acts as both a standalone weapon and a force multiplier in hybrid threats. Its ability to manipulate perceptions, distort realities, and exploit vulnerabilities makes it a highly effective tool in modern asymmetric conflicts.

---

[1] "Protecting the European elections from hybrid threats, including disinformation," Federal Ministry of the Interior and Community, June 6, 2024, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/european-election2024.html.
[2] Roberto Di Pietro, Simone Raponi, Maurantonio Caprolu, and Stefano Cresci, *New Dimensions of Information Warfare*, Advances in Information Security 84 (2021), 2.
[3] Roman Arutyunov, "Addressing Misinformation in Critical Infrastructure Security," *Dark Reading*, June 17, 2024, https://www.darkreading.com/cyber-risk/addressing-misinformation-in-critical-infrastructure-security.

Given the increasing threat of weaponized disinformation against corporations, research is needed on the current state of affairs. As Luke Tradinnick, the media scholar, has stated, "The issues associated with aggressive state actions in the information domain are not a hypothetical future threat, but are in a limited but clear way already part of international relations."[4] Therefore, this white paper explores the growing threat of weaponized disinformation targeting critical infrastructure, corporations, and societal stability. Leveraging real-world examples and hypothetical scenarios, the paper examines how disinformation can directly and indirectly harm critical infrastructure, such as power grids, transportation systems, and communications networks. It also investigates how disinformation can be used to incite violence and undermine corporate reputations. Despite weaponized disinformation's increasing prevalence, research on disinformation's impact on corporations remains limited, with most studies relying on simulations and surveys rather than real-world data. By analyzing documented incidents and proposing best practices, this paper aims to shed light on the strategies needed to prevent and respond to this emerging threat while highlighting the importance of further research to develop effective mitigation and resilience measures.

RELEVANT TERMS

Disinformation: False information deliberately created and disseminated to mislead, deceive, or manipulate an audience for strategic or malicious purposes. Disinformation often seeks to sow confusion, erode trust, or achieve political, social, or economic objectives.

Misinformation: False or inaccurate information shared without malicious intent. Unlike disinformation, misinformation is typically spread by individuals who believe the content to be true but lack the means or knowledge to verify its accuracy.

Malinformation: Information that is accurate but used maliciously to harm, manipulate, or discredit a person, group, organization, or nation. This includes releasing private or sensitive information (e.g., doxxing) or selectively disclosing facts out of context to create a false or misleading narrative.

[4] Luke Tredinnick, "(Dis)information warfare: Risks for businesses," *Business Information Review* 40, no. 3 (2023): 103-110.

Information Operations (IO): Coordinated actions designed to influence, disrupt, corrupt, or usurp the decision-making processes of a target audience. Information operations leverage the strategic use of information—whether true, false, or misleading—across various domains, including cyber, media, and psychological environments.

Influence Operations: A subset of information operations focused specifically on altering the opinions, behaviors, or decision-making of a target audience. Influence operations may use propaganda, manipulation, and other psychological techniques to achieve strategic objectives.

Narrative Attacks: Targeted efforts to undermine or distort widely accepted stories or perceptions that provide meaning, context, or legitimacy to a person, group, organization, or institution. Narrative attacks often exploit existing biases or grievances to reshape public understanding or erode trust.

Hybrid Threats: Complex and multifaceted threats that combine conventional military force with unconventional tactics such as cyberattacks, economic coercion, disinformation, and influence operations. Hybrid threats aim to exploit the vulnerabilities of a target by blending tools of warfare, espionage, and propaganda to achieve strategic objectives without triggering outright conflict.

Literature Review

Disinformation targeting critical infrastructure represents an emerging threat with profound implications for the functionality and resilience of societal systems. While research on this subject remains scarce, existing studies provide compelling evidence of the potential risks. Current research efforts predominantly rely on simulations and consumer behavior surveys, often exploring hypothetical scenarios rather than examining real-world incidents. This body of work underscores the significant vulnerabilities within energy, transportation, and supply chain systems, that adversaries can exploit using behavioral manipulation. By analyzing these studies, researchers can start to understand how disinformation can disrupt operational reliability, amplify systemic vulnerabilities, and create cascading effects on operations, supply chains, and public trust.

The most well-known of these studies is Raman et al. where the researchers found that "behavioral manipulation through disinformation can indeed lead to a full blackout in a heavily loaded grid."[5] Their research assessed a potential attack where adversaries manipulate citizens by sending fake discount notifications encouraging them to shift energy usage to peak-demand periods, potentially overloading power lines and causing blackouts. Using the power grid of Greater London as a case study, the research simulates residential energy consumer behavior, focusing on the impact of electric vehicle (EV) adoption. The analysis highlights the significant role EV charging plays in deferrable energy demand, which adversaries could exploit to cause greater disruption. The model explored varying EV adoption levels, and the grid capacity upgrades required to manage the corresponding demand, emphasizing how behavioral manipulation can exacerbate vulnerabilities in the power grid.

Through a survey of 5,124 participants via Amazon Mechanical Turk, the researchers assessed how people would respond to a notification offering a 50% electricity discount from 8 PM to 10 PM. Participants rated their likelihood to change their electricity usage patterns and forward the message to friends. The study examined two key factors influencing behavior. First, the notification sender in which notifications were either sent by a stranger (e.g., the attacker) or by a friend (via forwarding). Second, the notification content where one version required recipients to click an external link to claim the discount (phishing context) and another version offered the discount unconditionally (disinformation context). Using the survey data, they found that if the EV adoption rate in the power grid is 15% and then 30% of the population is initially targeted by an attacker, follow-through rates range from 9.4% to 26.8%. According to power grid simulations, these follow-through rates could cause blackouts affecting between 5.6% and 100% of residents. This provides direct evidence that influence operations could have a real impact on consumer behavior and impact critical infrastructure.

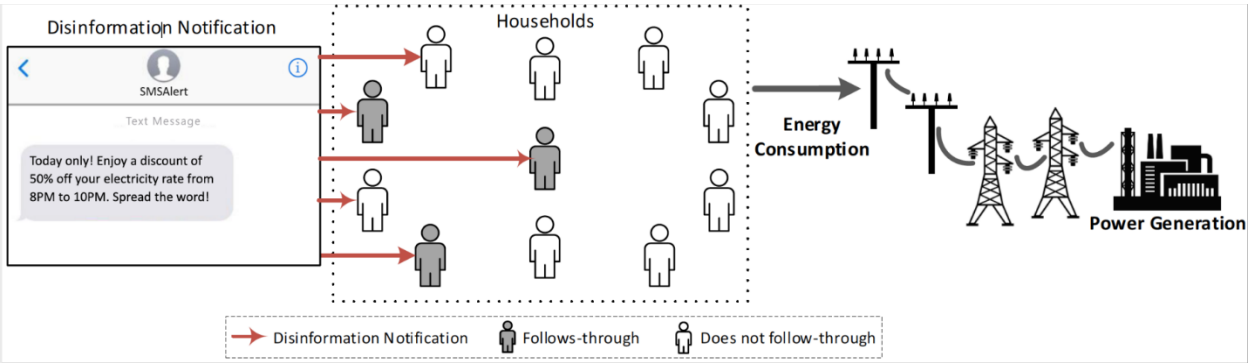


Image: Illustration of a disinformation attack on residential electricity consumers.[6]

[5] Gururaghav Raman, Bedoor AlShebli, Marcin Waniek, Talal Rahwan, and Jimmy Chih-Hsien PengI, "How weaponizing disinformation can bring down a city's power grid," PLoS One 15, no 8: e0236517, 7.
[6] "How disinformation can weaken infrastructure systems' resilience," ETH Zurich, August 19, 2020, https://frs.ethz.ch/news-events/frs-news-channel/2020/08/how-disinformation-can-weaken-infrastructure-systems-resilience.html.

A study by Ramin Khameneh, Kash Barker, and Jose Ramirez-Marquez examined how disinformation exacerbates disruptions in transportation infrastructure. The study focused on the Port Authority Trans-Hudson (PATH) system in New Jersey and New York.[7] By leveraging artificial intelligence techniques, it analyzed the operational impacts of disinformation-induced disruptions using data such as schedules, ridership reports, and real-time alerts. Their findings reveal that disinformation significantly impacts infrastructure reliability, causing extended downtime, station closures, and service rerouting. The study emphasizes the importance of robust strategies to mitigate disinformation's adverse effects, enhance operational responsiveness, and improve the resilience and public perception of transportation systems.

Similarly, Waniek et al. demonstrated the impact of disinformation on travel networks through a survey and simulation.[8] Their surveys assessed how individuals would respond to disinformation delivered via SMS alerts or road signs in divergence and convergence attacks. Participants started by rating their likelihood to follow SMS notifications like “Accident on ‘X’ Road. Please use alternative routes” on a 0-10 scale. According to the results, 89% reported a follow-through propensity of 6 or above for SMS alerts, and 97% reported a similar propensity for road signs stating, “ROAD AHEAD CLOSED.” In addition, 55% of participants reported a forwarding propensity of 6 or above, suggesting that while people are likely to act on such alerts, they are less inclined to share them with others.

The results indicate a high likelihood of behavior alteration due to disinformation. A significant majority of participants are likely to follow disinformation, particularly when presented as traffic alerts or road signs. As part of this, the trust in the sender's legitimacy, such as the label "SMSAlert," may contribute to the high follow-through rates. These results reveal a worrying potential for behavior alteration through disinformation, though the results may overestimate real-life actions.

Concerning their simulation, the evaluation of a divergence attack on 10 locations in Chicago revealed significant traffic disruptions. Using a simulation of one day's traffic, the attack was modeled to last 24 hours, with 50% of drivers responding to disinformation by rerouting. The chosen targets, selected by a greedy heuristic, were spread across the city and included both traffic directions at some locations. The attack caused noticeable changes in traffic patterns, diverting vehicles away from the targeted streets into neighboring areas, increasing traffic on some streets while reducing it on others. The effects extended beyond the immediate vicinity of the targets, impacting traffic flow citywide.

[7] Ramin Talebi Khameneh, Kash Barker, Jose Emmanuel Ramirez-Marquez, “A hybrid machine learning and simulation framework for modeling and understanding disinformation-induced disruptions in public transit systems,” *Reliability Engineering & System Safety* 255 (2025).
[8] Marcin Waniek, Gururaghav Raman, Bedoor AlShebli, Jimmy Chih-Hsien Peng, Talal Rahwan, “Traffic networks are vulnerable to disinformation,” *Scientific Reports* 11, 5329 (2021).

Jamalzadeh et al. (2022) proposed a disinformation tracking model that integrates an epidemiological SIR model and an electric power network optimization model to analyze and mitigate the impact of disinformation on electric power networks.[9] The research focused on identifying vulnerable power nodes and countering disinformation by disseminating accurate information to targeted communities. The model is demonstrated using a large-scale electric power network in Los Angeles County, California. Key findings highlight how adversaries can disrupt critical infrastructures and how monitoring the intensity and duration of disinformation can help manage infrastructure performance and counter disinformation. The methodology is adaptable to other infrastructure networks, such as gas pipelines and transportation systems, with appropriate modifications to account for specific physical flow constraints. However, the model's limitations include the need to define network boundaries for computational feasibility, as power networks are interconnected.

Jamalzadeh et al. (2024) looked at the impact of disinformation on Sweden's railway network in 2015, focusing on supply and demand for 14 commodities transported between 1,363 stations.[10] Using a multi-commodity disinformation model, they found that disinformation targeting high-importance commodities (e.g., wood, cork, pulp, paper) can lead to shortages of less critical commodities (e.g., ore) as resources are reallocated to meet higher-priority demands. Severe shortages occur when the rate of disinformation spread significantly exceeds the rate of recovery or countermeasures. Shortages peak differently across commodities based on disinformation spread and recovery rates. Wood, cork, pulp, paper shortages peak rapidly in high-volume attacks, while shortages for ore and other non-metallic minerals remain steady over time. The transportation system prioritizes critical commodities during disinformation-induced disruptions, but this leads to persistent shortages in less critical commodities. This study highlights the vulnerability of interconnected supply chains to disinformation and emphasizes the need for effective countermeasures to minimize economic and operational impacts. Importantly, they argued that "[w]ith the number of social media platforms and users increasing daily, it has become easier to create and distribute false information, which may ultimately harm physical systems and infrastructure."[11]

The studies presented reveal the alarming potential of disinformation to disrupt critical infrastructure through behavioral manipulation and systemic exploitation. From power grids to transportation networks and supply chains, adversaries can use disinformation to induce significant operational disruptions, as evidenced by survey-based behavioral analyses and simulation results. Despite these insights, the over-reliance on hypothetical scenarios leaves a critical gap in understanding real-world dynamics. By investigating real-world responses,

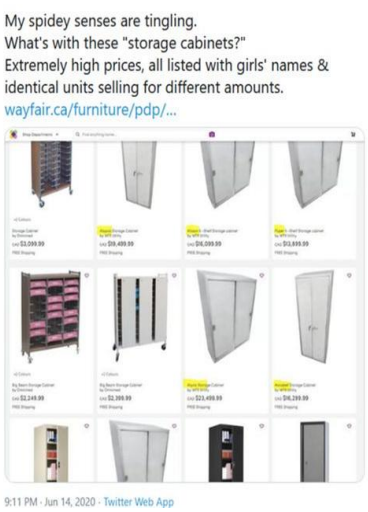
[9] Saeed Jamalzadeh, Kash Barker, Andrés D. González, and Sridhar Radhakrishnan, "Protecting infrastructure performance from disinformation attacks," *Scientific Reports* 12(1):12707 (2022).
[10] Saeed Jamalzadeha, Lily Mettenbrinka, Kash Barkera, Andrés D. Gonzálezaa, Sridhar Radhakrishnanb, Jonas Johanssonc, and Elena Bessarabova, "Weaponized disinformation spread and its impact on multi-commodity critical infrastructure networks," *Reliability Engineering & System Safety* 243 (2024).
[11] Ibid, 7.

mitigation strategies can be refined to enhance infrastructure resilience and public trust, ensuring a proactive stance against this escalating threat.

Examples of Disinformation Impacting Businesses

The threat of weaponized disinformation to corporations is multifaceted, ranging from bizarre conspiracies to targeted political attacks and even market manipulation. These campaigns can erode trust, damage reputations, and cause financial harm, regardless of whether the targeted organization is a multinational corporation or a small business.

In some cases, disinformation manifests as wild conspiracies, often rooted in fringe online communities. For example, in 2020, the furniture retailer Wayfair became entangled in a baseless conspiracy propagated by QAnon supporters.[12] They claimed that Wayfair's product listings—specifically items with disparate prices—were coded messages for child trafficking operations. The real explanation for the pricing differences was a computer glitch, but the conspiracists further inflamed the issue by falsely associating furniture names with actual missing persons. Similarly, in 2017, right-wing users on 4Chan launched a politically motivated disinformation campaign against Starbucks.[13] They circulated a fake flier claiming Starbucks was offering undocumented immigrants a 40% discount, a ploy seemingly designed to stoke public outrage after the company had pledged to hire 10,000 refugees. Although these examples generated online controversy, they primarily caused reputational challenges rather than financial losses.



Images: Left – The Wayfair conspiracy on social media. Right – The fake Starbucks flier.

However, disinformation can also have direct market implications. In 2018, a fake memo claimed that the Pentagon had requested a national security review of Broadcom's acquisition of CA Technologies, allegedly under the purview of the Committee on Foreign Investment in

[12] Marianna Spirng, "Wayfair: The false conspiracy about a furniture firm and child trafficking," BBC, July 15, 2020, https://www.bbc.com/news/world-53416247.
[13] Cydney Henderson, "That starbucks 'ad' promising discounts for undocumented immigrants is fake," *AZ Central*, August 9, 2027, https://www.azcentral.com/story/news/nation/2017/08/09/z-starbucks-shoots-down-fake-ad-promises-discounts-undocumented-immigrants/552044001/.

the United States (CFIUS).[14] The rumor caused both companies' stocks to drop significantly and led Broadcom to relocate its headquarters back to the United States, a move aimed at avoiding potential regulatory scrutiny. Similarly, in 2019, false rumors spread on WhatsApp triggered a panic-driven run on Metro Bank, severely impacting its stock price.[15] The bank was already under pressure from an earlier accounting error, and the disinformation exacerbated investor fears, resulting in significant financial losses.

Small businesses are not immune to the pernicious effects of disinformation, which often takes an even more malicious form in these cases. In 2017, a prank website published a fabricated story accusing the Indian restaurant Karri Twist of serving human flesh.[16] This outrageous claim not only hurt the restaurant financially but also provoked threats of violence, with some individuals suggesting the business should be bombed. More recently, in 2023, a fake Reddit post purportedly from a disgruntled employee accused the sports card company Backyard Breaks of committing fraud.[17] Although the post was swiftly removed, it caused the company to curtail its purchases of expensive sports cards, which subsequently hurt sellers in the sports memorabilia market.

These cases illustrate the diverse and harmful ways disinformation can target corporations. From conspiracy theories to orchestrated market manipulation, the consequences can range from reputational damage to severe financial losses. As these examples demonstrate, disinformation campaigns, whether motivated by political agendas, financial gain, or sheer malice, pose a significant threat to businesses generally.

Violence and Reputation

The intersection of conspiracies, political issues, and disinformation with corporate reputation can escalate to threats or acts of violence, highlighting the critical need for security professionals to address the risks of corporate reputation warfare. These incidents demonstrate that the consequences of disinformation extend far beyond financial losses or reputational damage—they can endanger lives and disrupt operations.

---

[14] "Pentagon says memo asking for Broadcom-CA deal review is likely fake," *Reuters*, October 10, 2018, https://www.reuters.com/article/us-ca-technologies-m-a-broadcom/pentagon-says-memo-asking-for-broadcom-ca-deal-review-is-likely-fake-idUSKCN1MK26J/.

[15] Kalyeena Makortoff, Miles Brignall, and Jim Waterson, "Metro Bank shares plunge as it attacks 'false rumours'," *The Guardian*, May 13, 2019, https://www.theguardian.com/business/2019/may/13/metro-bank-shares-rumours-safety-deposit-boxes.

[16] "Indian restaurant told they 'should be bombed' over fake news about serving human meat," CBC Radio, May 30, 2017, https://www.cbc.ca/radio/asithappens/as-it-happens-tuesday-edition-1.4137713/indian-restaurant-told-they-should-be-bombed-over-fake-news-about-serving-human-meat-1.4137715.

[17] Mario Alejandro (@BeisbolCardBlog), "On @Reddit, a former employee of Backyard Breaks has posted an anonymous thread going into details on how BB is committing fraud against collectors in #thehobby.," X, September 14, 2023, https://x.com/BeisbolCardBlog/status/1702271237718741170.

One prominent example is the 2020 Nashville bombing, where conspiracy theories partly motivated the perpetrator to target an AT&T building.[18] The following year, law enforcement thwarted a potentially devastating attack when Seth Aaron Pendley attempted to procure explosives to bomb an Amazon data center.[19] Pendley's motivations were rooted in a conspiratorial view of the company as part of a broader oligarchy he sought to undermine. These cases illustrate how conspiracy theories about corporations, particularly those perceived as politically influential, can lead to direct threats of violence.

However, corporations are also impacted by conspiracies that extend beyond their own operations. For example, the rise of right-wing terrorism has been fueled by conspiratorial ideologies, such as the Great Replacement theory. In 2019, Patrick Crusius cited this theory as his motivation for attacking a Walmart in El Paso, Texas, intending to kill as many Mexicans and immigrants as possible.[20] While Walmart itself was not the primary target of Crusius' ideology, its presence in a border community made it a site of violence, demonstrating how corporations can become indirect victims of broader societal conspiracies.

Political stances, or even perceptions of political stances, can also provoke threats. In 2023, Anheuser-Busch faced backlash and bomb threats after a partnership with a transgender influencer sparked controversy among certain right-wing groups.[21] Similarly, Target received bomb threats from individuals on both sides of the LGBTQ+ debate.[22] In one instance, Target was targeted for being "insufficiently pro-LGBTQ" after removing or relocating a children's pro-trans clothing line in response to right-wing criticism.[23] These events underscore how polarizing political and social issues can make corporations lightning rods for violent threats.

Misinformation, distinct from conspiracies or politics, also poses a threat. In 2022, misinformation about electric vehicle company Faraday Future allegedly filing for bankruptcy not only hindered its ability to secure investment but also led to death threats against its board members.[24] This example highlights how even seemingly mundane disinformation can escalate into personal safety risks for corporate leaders.

---

[18] "FBI Releases Report on Nashville Bombing," FBI, March 15, 2021, https://www.fbi.gov/contact-us/field-offices/nashville/news/fbi-releases-report-on-nashville-bombing.
[19] Phil Helsel, "Texas man who wanted to blow up Amazon data center sentenced to 10 years," *NBC News*, October 1, 2021, https://www.nbcnews.com/news/us-news/texas-man-who-wanted-blow-amazon-data-center-sentenced-10-n1280615.
[20] Ashley Killough, "El Paso Walmart shooter agrees to pay more than $5.5 million in restitution in federal case," CNN, September 25, 2023, https://www.cnn.com/2023/09/25/us/el-paso-walmart-shooter-millions-restitution/index.html.
[21] Danielle Wiener-Bronner, "Anheuser-Busch facilities face threats after Bud Light backlash," CNN, April 20, 2023, https://www.cnn.com/2023/04/20/business/bud-light-threats/index.html.
[22] Olafimihan Shin, "Target stores in at least five states receive bomb threats over Pride items," *The HillI,* June 12, 2023, https://thehill.com/homenews/state-watch/4046688-target-stores-in-at-least-five-states-receive-bomb-threats-over-pride-items/.
[23] Brian Flood, "Target stores reportedly received bomb threats for LGBTQ community betrayal," *NY Post*, June 13, 2023, https://nypost.com/2023/06/13/target-stores-reportedly-received-bomb-threats-for-betraying-lgbtq-community/.
[24] Andrei Nedelea, "Faraday Future Execs Received Death Threats As Production Start Nears," *Inside EVs*, September 23, 2022, https://insideevs.com/news/612241/faraday-future-board-members-death-threats/.

These incidents demonstrate the severe consequences that conspiracies, political controversy, and misinformation can have on corporations, from direct attacks to threats against employees and disruptions to operations. Security professionals must recognize that these risks are not just reputational but also physical, requiring proactive measures to monitor, mitigate, and respond to disinformation and its potential consequences. By addressing these challenges head-on, corporations can better protect their employees, facilities, and reputations in an increasingly volatile landscape.

Online Information Space, Radicalization, and Terrorism

Part of the puzzle of weaponized disinformation and critical infrastructure security lies in the intersection of the online information space and targeted violence. The examples above gave direct evidence of disinformation leading to at least threats of violence, but research focused on the far-right shows how online community dynamics contribute to the adoption of militant accelerationist ideology and the promotion of critical infrastructure attacks within extremist communities. Saddiq Basha identified two key patterns influencing such behavior: the role of far-right online influencers and peer-to-peer encouragement.[25]

According to his research, influencers use parasocial relationships—one-sided, non-reciprocal connections—to shape followers' views and mobilize support for extremist ideologies. These influencers build trust through consistent content production, active engagement, and symbolic gestures, such as acknowledging their followers' interactions with their work. Examples include figures like Mike Ma, who popularized militant accelerationism through his writings and social media presence. Even after his account was suspended, his content continued circulating in extremist groups, reinforcing his influence.

In extremist online communities, like-minded individuals also foster trust and encourage radical behavior through direct interactions. Normative conformity, as explained by Social Identity Theory, pushes members to adopt the group's extremist values, particularly those who see themselves as peripheral members. Members of these groups actively share radical content, including manifestos, tactical manuals, and propaganda advocating attacks on critical infrastructure. They also frequently engage in discussions to normalize and celebrate these actions. Real-world cases illustrate this dynamic, such as three U.S. men who plotted to attack power grids after connecting in online chat groups, where one initially proposed the idea and recruited others using neo-Nazi materials.

Online platforms enable both influencers and peers to propagate accelerationist ideologies, normalize critical infrastructure attacks, and recruit adherents. This highlights the significant

[25] Saddiq Basha, "Death to the Grid: Ideological Narratives and Online Community Dynamics in Encouraging Far-Right Extremist Attacks on Critical Infrastructure," *Counter Terrorist Trends and Analysis* 15, no. 4 (2023): 17-24.

role of online community dynamics in fostering radicalization and facilitating extremist actions, and this type of information space is likely to play an important role in weaponized disinformation against critical infrastructure.

Examples of Disinformation Impacting Infrastructure

After examining examples of disinformation's negative impact on businesses and its potential to incite violence specifically, it is time to explore the available examples of disinformation impacting critical infrastructure.

The first example occurred when two Israeli software engineering students, Shir Yadid and Meital Ben-Sinai, successfully created a fake traffic jam on the GPS and traffic app Waze as part of a university project at the Israel Institute of Technology.[26] Using an Android emulator and scripting, they generated numerous fake accounts and false GPS data to mimic congestion, which Waze then reported as a real traffic jam. The experiment was limited to a quiet back road within their campus to avoid real-world disruptions. Their faculty advisor, Professor Eran Yahav, emphasized that their goal was to highlight vulnerabilities in Waze's system and explore defense mechanisms against such Sybil attacks.[27] They promptly informed Waze of their findings and shared their academic paper detailing the research. The hack required minimal resources, did not involve breaching Waze servers, and was conducted ethically. Waze, owned by Google, acknowledged the issue and pledged to address it. The project demonstrated both the feasibility of such attacks and potential solutions to safeguard against them.

A similar "attack" took place when artist Simon Weckert conducted a project called the Google Maps Hack, demonstrating how easily Google Maps' traffic system can be manipulated.[28] Inspired by noticing false traffic jams caused by large crowds at a Berlin protest, Weckert acquired 99 smartphones, placed them in a red wagon, and walked through Berlin streets. The phones, transmitting GPS data, tricked Google Maps into displaying non-existent traffic congestion. Weckert's experiment pointed to vulnerabilities in Google Maps and raised questions about how technology influences society. He emphasized that his project wasn't a prank but a way to explore the relationship between technology and the physical world. By fabricating traffic jams, he showcased how Google Maps could redirect vehicles to other routes, potentially straining infrastructure. Weckert also used the project to critique the

[26] Nicholas Tufnell, "Students hack Waze, send in army of traffic bots," *Wired*, March 25, 2014, https://www.wired.com/story/waze-hacked-fake-traffic-jam/.
[27] A Sybil attack in one that involves forging multiple identities to target a network. Named after the famous character from the 1976 TV miniseries *Sybil*.
[28] Brian Barrett, "An Artist Used 99 Phones to Fake a Google Maps Traffic Jam," *Wired*, February 3, 2020, https://www.wired.com/story/99-phones-fake-google-maps-traffic-jam/?_sp=6b141631-46d7-44e9-bfba-bb3246ea39ab.1734904325678.

opaque nature of tech systems and their societal impact, particularly focusing on issues like gentrification and urban infrastructure. Although initially overlooked, the project gained viral attention after a tweet, reminding users of the manipulability and inherent biases in systems they rely on daily.

Waniek et al.'s study emphasizes why such fake traffic alerts could be extremely impactful.[29] First, people are highly likely to act on fake traffic alerts, given the seemingly harmless nature of these notifications compared to phishing or spam, which seek sensitive information. Second, the disruptive impact of such disinformation underscores the need for effective detection and countermeasures. One potential solution is crowdsourced verification, leveraging input from individuals near the reported incident, as crowdsourced fact-checking has proven effective in assessing news reliability. However, among widely used navigation apps, only Waze currently offers such functionality, with an estimated 11% market share in the U.S.

While not intended as an attack, the following example shows how inaccurate information can cause real delays. In 2020, Rashidul Islam made a fake bomb threat to delay an EasyJet flight from London to Marrakech so he could catch it after running late.[30] He called the threat in from his own cell phone, leading to passengers and crew being evacuated and delayed for three hours while authorities investigated. Upon arriving at the airport, Islam was apprehended when police matched the anonymous threat to his phone number. If that information had been spread on social media, then it is extremely likely that the airport would have had to shut down, causing widespread delays affecting thousands of passengers.

Scenarios of Weaponized Disinformation

The scarcity of real-world case studies on weaponized disinformation targeting critical infrastructure necessitates the use of hypothetical scenarios and simulations to explore potential risks. While such models may lack the unpredictability of real-world events, they allow researchers and practitioners to anticipate vulnerabilities and devise mitigation strategies. The following scenarios, inspired by the documented examples, demonstrate how disinformation can disrupt critical systems and pose significant security risks. These hypothetical situations are rooted in existing trends and incidents, offering a realistic framework for understanding the potential consequences of disinformation on urban traffic systems and communications networks.

[29] Waniek et. al., np.
[30] Rich Thomaselli, "Man Tries to Delay Flight by Reporting Fake Bomb Threat," *Travel Pulse,* January 18, 2020, https://www.travelpulse.com/news/airlines-airports/man-tries-to-delay-flight-by-reporting-fake-bomb-threat.

Scenario 1: Disinformation Targeting Traffic During a Major Event

Imagine a bustling metropolitan city hosting a high-profile international summit. The event attracts global leaders, media, and thousands of attendees, placing immense pressure on the city's transportation infrastructure. A coordinated disinformation campaign emerges on social media, disseminating fake traffic alerts through posts mimicking the official city transit authority. These alerts falsely claim that key roads near the summit venue are closed due to security threats, directing drivers to alternative routes that quickly become overwhelmed with diverted traffic.

Simultaneously, digital billboards are hacked to display fake messages reinforcing the closures, while doctored videos circulate showing emergency responders at supposedly blocked intersections. The combination of false information creates chaos, causing gridlock across the city. Public transportation becomes overcrowded as commuters abandon their cars, and emergency services struggle to reach critical areas due to the congestion.

The disruption leads to delays in summit proceedings, significant economic losses for local businesses dependent on event traffic, and mounting public frustration. Although the disinformation is eventually identified and countered, the response is slow due to the sheer scale of the operation and the difficulty in verifying legitimate communications during the crisis.

Scenario 2: Misinformation Inspiring a Terrorist Attack on a Communications Network

In this scenario, a prominent telecommunications company is accused in a disinformation campaign of participating in a government surveillance program. The claims, fueled by deepfake videos and manipulated internal documents shared on fringe online forums, spread rapidly among conspiracy theorists and anti-government groups. One such individual, already radicalized by right-wing extremist propaganda, becomes convinced that the company is a core component of a "globalist" agenda.

Acting on these beliefs, the individual plans an attack on one of the company’s regional data centers, which serves as a hub for internet connectivity in a multi-state area. The perpetrator creates homemade explosives and uses information gleaned from publicly available building blueprints to target critical infrastructure within the facility.

The attack results in partial damage to the data center, causing widespread internet outages and communication disruptions in the region. Emergency services, hospitals, and businesses relying on internet connectivity are particularly affected, exacerbating the impact. Although the attacker is apprehended shortly after the incident, the recovery and restoration of services take days, leading to significant economic losses and undermining public trust in digital infrastructure security.

These scenarios underscore the serious risks posed by weaponized disinformation to critical infrastructure, even in the absence of extensive real-world examples.

Initial Assessment of Best Practices

By examining these hypotheticals and the available real-world examples, researchers can draw valuable lessons on how to mitigate such threats. The following serves as a starting point for best practices and recommendations to prevent and respond to weaponized disinformation targeting critical infrastructure. Organizations will need to assess their own resources and capabilities to implement these effectively.[31]

BEST PRACTICES AND RECOMMENDATIONS

1. **Secure Leadership Commitment**

- Convince executives such as the CEO, CISO, and/or CSO of the importance of defending against disinformation.
- Leadership commitment ensures the allocation of necessary resources and empowers stakeholders to act decisively.

2. **Assign Responsibility**

- Designate a leader or team with clear ownership of prevention, mitigation, and response strategies. Importantly, this will need to be a multidisciplinary approach, and the aforementioned lead person/team will need to draw on multiple areas of expertise.
- Ensure this team develops actionable, results-oriented policies.

3. **Develop a Robust Communication Plan**

- Create communication templates for responding to media inquiries, employee concerns, and vendor questions.
- Consider retaining a communications firm for rapid response during crises or high-risk situations.

4. **Build and Maintain a Trusted Reputation**

- Invest in programs that enhance internal and external reputations through consistent, transparent communication.

[31] These lessons are not only drawn from the examples, scenarios, literature, and corporate documents. See Tredinnick (2023); Bank of America, "The threat misinformation and disinformation pose to business," *Cyber Security Journal* 7 (2023), https://business.bofa.com/content/dam/flagship/global-transaction-services/misinformation/Misinformation.pdf; Ika Trijsburg, Helen Sullivan, Elise Park, Matteo Bonotti, Paul Costello, Zim Nwokora, Daniel Pejic, Mario Peucker, and Wiliam Ridge, "Disinformation in the City Response Playbook," German Marshall Fund/University of Melbourne (2024).

5. **Implement Monitoring and Threat Intelligence**

- Designate intelligence analysts to monitor the broader risk context and identify early warnings, including sentiment analysis and extremist forums.
- Use search alerts to track mentions of your company, services, and employees across online platforms to identify unusual or negative references.
- Evaluate AI and machine learning tools to scan social media for falsified information, including manipulated video or audio.

6. **Secure Social Media Presence**

- Set up verified profiles on all major social media platforms, including emerging ones, to protect against spoofing.

7. **Conduct Regular Tabletop Exercises**

- Develop drills simulating mis- or disinformation incidents to test responses impacting customers, employees, and stakeholders.
- Assign roles, establish communication trees, and ensure emergency contacts are available on weekends and after-hours.

8. **Prepare Templates and Messaging**

- Draft templates for press releases that quickly counter false claims with updated and verified information.
- Cultivate relationships with journalists, influencers, and other trusted voices who can help mitigate disinformation in real time.

9. **Integrate Critical Information into Risk Registers**

- Identify and classify business-critical information assets and resources that are vulnerable to disinformation attacks.
- Plan protective measures to prevent disruptions to communications networks and access to vital information.

10. **Incident Response Planning**

- Involve relevant stakeholders from inside and outside of security teams in crafting incident response plans.
- Address the organization's specific needs and vulnerabilities in response to information-based threats.