Corporate Reputation Warfare

DISINFORMATION, POLARIZATION, AND THE MARKETPLACE

IF Insight Forward

Key Takeaways

- The same kinds of information operations used in domestic politics, foreign policy, and geopolitics are now being used to directly target corporations.
- They are carried out by nation-states, competitors, and malicious ideologically opposed groups and individuals.
- Advances in technology are making it easier and cheaper to create highly realistic and effective mis- and disinformation campaigns
- Corporations are vulnerable because of stakeholder expectations of corporate action on ESG issues, political polarization, and an increased scrutiny of corporate and executive behavior.
- Disinformation campaigns can directly damage a corporation's reputation, which has negative impacts on market share, stock price, and the ability to attract and retain employees.
- They can also result in employee activism, protests, and even threats and acts of physical violence.
- IF assess that **'corporate reputation warfare'** will be an important risk over the long term.

Corporate Reputation Warfare: Disinformation, Polarization, and the Marketplace

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 in declaring war against Spain in 1898. During the Cold War, the Soviet Union spread malicious conspiracies about the US, such as America inventing the AIDS virus. The US 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 information 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. **All of this is really about reputation and how a corporation's reputation impacts their business.**

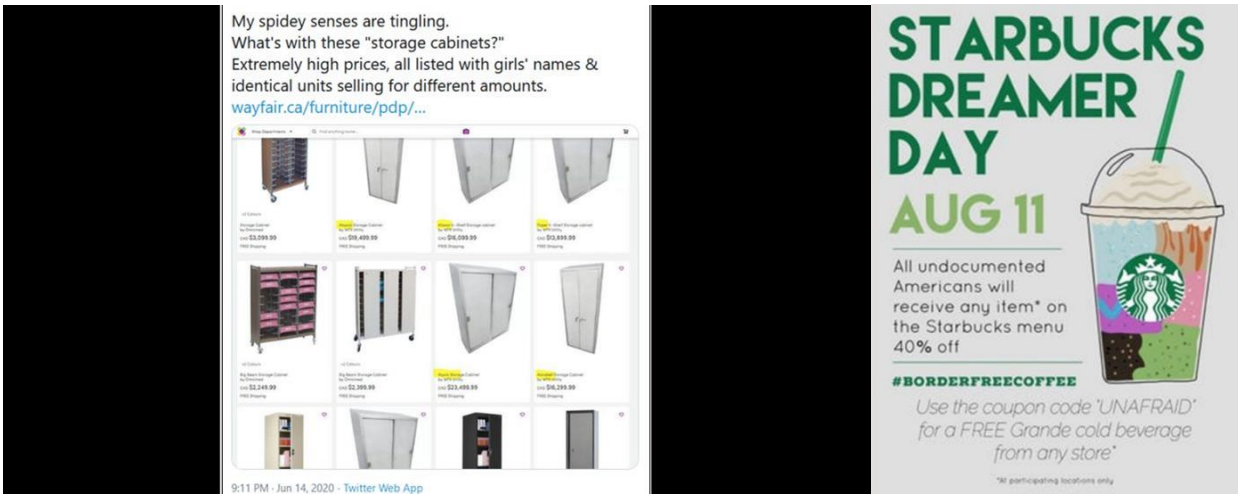
There are several reasons that corporations are becoming targets of conspiracies. First is the increasing influence corporations and high net worth individuals have on the political space. This does not necessarily mean directly influencing policy, but their prominent role in socio-political issues has made them targets. Bill Gates, the founder of Microsoft, is regularly connected to conspiracy theories. During the Covid pandemic, a conspiracy spread that he was part of a "cabal" that helped create and spread the virus so the elites could put microchips in people via the vaccine that would be activated by 5G. Second, people are becoming incredibly suspicious about those in power and ascribing to them motives and capabilities they do not really have. The 2023 Edelman Trust Barometer documents the declining trust in institutions in the United States, and that lack of trust means people will refuse to believe information given by those institutions. Finally, the deep polarization occurring in the US also impacts people's willingness to believe information and their willingness to purchase products from corporations.

> **Corporate reputation warfare is when private firms must contend with dis- and misinformation about their business or executives OR the fallout of taking or perceiving to take political stances on controversial or sensitive issues.**

Insight Forward assesses that disinformation and polarization concerning brand reputation or what we would term "Corporate Reputation Warfare" is a significant risk to businesses. Corporations will have to contend with conspiracies about their leaders and products while simultaneously managing their public stances on political issues. Understanding this issue will be critical to managing market and security risks for corporations as businesses attempt to control the narrative around their brands.

Recent Examples of Disinformation about Businesses

The threat to corporations from weaponized information can range from paranoid conspiracies to political attacks and market sabotage. In 2020, the furniture company Wayfair had to deal with a peculiar conspiracy stemming from the QAnon community in which supporters claimed Wayfair's ads were secretly describing children to be trafficked due to disparate prices for furniture (the real reason the prices were different was a computer glitch). QAnon supporters on Reddit also incorrectly linked the furniture names with actual missing persons. In 2017, right-wingers on 4Chan wanted to troll Starbucks, so they created a fake flier detailing how the company would give undocumented immigrants a 40% discount on their orders. Social media fury ensued, but the flier was entirely made up. This was likely done because that same year Starbucks had pledged to hire 10,000 refugees, which the political right opposed.



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

While those examples led to disagreements online, there have been real market impacts from false information. In 2018, a fake memo of unknown origin claimed that the Pentagon asked for a national security review by The Committee on Foreign Investment in the United States (CFIUS) of Broadcom purchasing CA Technologies. This not only led to a major slide in the stock of both companies, but Broadcom also returned its headquarters to the US to prevent even the possibilities of such reviews. In 2019, Metro Bank's shares plummeted because of false rumors spread on WhatsApp advocating a run on the bank. Metro had problems earlier that year due to an accounting error, and investors were already nervous about the financial stability of the UK-based bank.

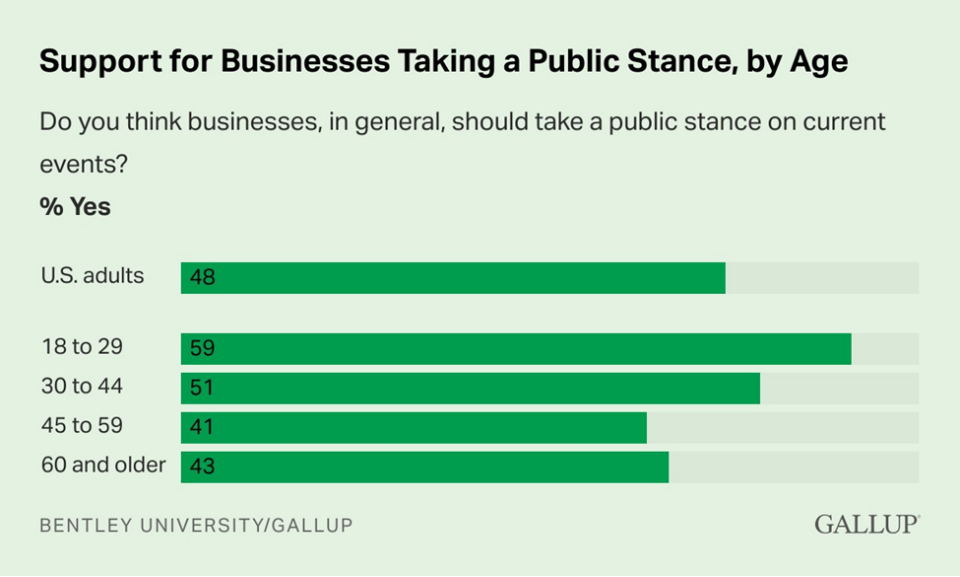
There are also several examples of disinformation harming small businesses. These tend to be far more malicious in nature. In 2017, a prank website published a fake story claiming the long-time Indian restaurant Karri Twist engaged in anthropophagy by serving their customers human flesh. Not only did the business suffer economically, but people declared the restaurant should be bombed. In September 2023, a fake employee posted on Reddit to say negative things about Backyard Breaks (a sports card company), claiming the company was committing fraud. The post

was quickly taken down, but it led Backyard to stop purchasing expensive cards, which harmed sports paraphernalia sellers.

Consumers and Politics: What does the market want?

Disinformation, misinformation, and fake news stories can have real deleterious impacts on businesses, but that is not the only type of corporate reputation warfare that occurs. Corporations also face political risk from consumers making purchasing decisions based on their ideological views. However, the issue is complicated because not all consumers base decisions on politics, and there is even a sizable part of the market that does not want corporations to be political.

Gallup released a survey in January 2023 showing that the public is fairly split on this topic: 48% of consumers want businesses to take public stances on issues while 52% of consumers said they should not. Importantly, younger consumers are more likely to support businesses taking political stances as the survey found "59% of those aged 18 to 29 think as much, compared with 51% of those aged 30 to 44, 41% of those aged 45 to 59, and 43% of those aged 60 and older." This also impacts the market because of which generation has purchasing power. Older consumers currently have more purchasing power, and they are less likely to support businesses being political. Yet those who *will* have purchasing power in a few years are more likely to want businesses to be political. Corporations will have to navigate the current versus future market when making these decisions.



The Gallup survey also found that Democrats are significantly more likely to want businesses to be political (75% compared to 18% for Republicans). In a different survey, the communications firm Edelman found that 64% of consumers will buy or boycott a brand only because of that company's political positions. The data therefore shows both opportunities and risks in corporations being political. Some businesses have found themselves appealing directly to left-wing consumers as a means to have a larger part of the market share. For example, the women's

workwear brand Argent chose to sell hot pink power suits by partnering with Supermajority (a women-focused voter outreach organization). Argent donated 10% of sales revenue from the suits to Supermajority during the 2020 election, and the suits sold out within a day. Right-wing companies have also found similar success by focusing on consumers who agree with them politically. Black Rifle Coffee Company has found success appealing to the political right by overtly supporting law enforcement, veterans, and firearm rights, though the company lost out with some on the right when they distanced themselves from extremists.

Consumers and Politics: Backlash, Boycotts, and Bills

Gaining market share by being overtly political works in certain contexts, but other companies have suffered tremendously for doing so. Most infamously this year, Budweiser partnered with trans influencer Dylan Mulvaney for March Madness. Consumers unhappy with the partnership responded with a massive boycott of the company. Unlike other boycotts, this one worked. From April-June 2023, Anheuser-Busch Inbev (the maker of Budweiser) saw revenue drop 10.5% in the United States. Sales of Budweiser plummeted by more than a quarter, and those sales still have not returned.

A boycott of Budweiser was one response, but Disney faced more direct government blowback from its overt political stances. Florida Governor Ron DeSantis took actions against Disney after the company criticized the governor's parental rights bill (critics refer to the legislation as the "don't say gay" bill). DeSantis instigated a dispute over taxes and land use, and Disney then cancelled a major project in the state. **Corporate reputation warfare over partisan politics can harm corporations when consumers and governments attempt to punish businesses over their stances.**

It is not just governments and consumers that create political risks for businesses. Employees are increasingly engaging in activism against company policies that they do not agree with. Employees in critical sectors tend to be significantly more left-wing than the executive leadership, and such political employees put demands on their corporations. *Vox* has collected relevant data that shows tech employees are overwhelmingly left-wing, which has impacted major technology firms on important projects. At Microsoft, employees protested the company working with US Immigration and Customs Enforcement, though that was a minor protest in comparison to others. Google had to entirely abandon a project with the government called Project Maven that would have used AI to help drones distinguish between threats and civilians after employees refused to work on any tool of war. Google employees are now protesting the work the company does with Israel on defense issues.

Defense issues and the tech sector are not the only examples of employees protesting over the politics of a company. In Los Angeles, employees at a Cinnabon walked out because of the company's prohibition on Pride décor. Workers at multiple Starbucks went on strike over a similar issue of locations taking down Pride flags. Neither Cinnabon nor Starbucks opposed

Pride month, but by trying to manage their reputation with consumers some employees took action to make the companies decisions appear more political.

Violence and Reputation

Conspiracies and political issues for corporations can actually lead to violence or the threat of violence, which is why security professionals must care about corporate reputation warfare. Typically, Pizzagate is held up as a prime example, but there are several others that raise concern. In 2020, conspiracy theories were found to be a partial motivation for a suicide bombing in Nashville, TN that targeted an AT&T building. The following year, the FBI apprehended would-be terrorist Seth Aaron Pendley before an attack could occur. Law enforcement intervened early when Pendley attempted to buy explosives. Pendley wanted to bomb an Amazon data center in the hopes of disrupting the internet and bringing down the "the oligarchy." His motivations were rooted in perceptions of the technology company's influence on socio-political issues.

Corporations are not only impacted by conspiracies about the company itself. The recent increase in right-wing terrorism connects to a symbiotic rise of conspiracies. Some terrorists use those conspiracies as justification for their violence. In 2019, Patrick Crusius attacked a Walmart in El Paso, Texas because of his beliefs around the Great Replacement conspiracy that holds elites in the West are deliberately bringing non-white immigrants to the US and Europe to replace white people. Crusius wanted to kill as many Mexicans and immigrants in the border town as possible. Risks from conspiracies can sometimes be indirect, and corporations that operate even tangentially to those areas can become targets or be impacted.

Threats of violence can also come from a corporation's public political stances (or perceptions about their political stances). Following the controversy Anheuser-Busch had with trans influencer Mulvaney, the company received threats that forced them to close some facilities for the safety of workers. One facility in Los Angeles even received a bomb threat. Around the same time, Target was also the recipient of bomb threats over LGBTQ issues, but the alleged perpetrator was angry that Target was insufficiently pro-LGBTQ. In spring 2023, Target established a pro-trans line of clothing for children that some right-wing persons believed was grooming behavior. After removing the clothes (or simply putting them in the back of stores), an anonymous person emailed a bomb threat to stores in five states because Target "betrayed the LGBTQ+ community."

Sometimes threats are due to misinformation, not just conspiracies or politics. In 2022, Electric vehicle company Faraday Future reported that it was unable to raise investment funds because of misinformation about the company filing for bankruptcy. The issue resulted in some board members receiving death threats.

Outlook

Advances in technology have made it easier and cheaper to create highly realistic audio, video, images, and text. This will facilitate the creation of even more sophisticated mis- and disinformation campaigns and further increases the risk of corporations being directly and successfully targeted. The risks are highest for businesses that take very public stances on political or social issues or that have outspoken executives. However, other businesses should be aware of the increased scrutiny of corporate behavior in general. As companies adopt more policies related to ESG issues, they face closer examination of their conduct and malicious actors are increasingly likely to exploit company policies against them.

Managing Risks from Corporate Reputation Warfare

Intelligence analysts and security professionals can prepare to help manage corporate reputation warfare from disinformation, conspiracies, and political issues by focusing on detection and working with business partners. The following are some suggested steps to take to help deal with these issues.

1. Decide as a corporation whether political issues will be part of corporate values or not. If they are going to be, then corporations will need to accept how widely they will publicize policies and stances and the increased risks from doing so.
2. Establish policies for how employees and executives should share their opinions on sensitive subjects. This does not mean controlling speech outside of work, but corporations should determine what employees and executives can say while representing the company.
3. Build a regular meeting cadence with the communications and marketing teams to help explain possible risks and threats when the company decides to engage in political issues or do certain marketing campaigns. This is not to interfere in business decisions; it is to help the corporation understand and possibly prepare for threats if they want to take certain stances.
4. Create an appropriate monitoring structure for reputational issues that could become threats to the company.
    a. CEOs and other executives often become the focal point for brand and reputation issues. Security teams should specifically monitor how the organization, its CEO, and other executives are being discussed online, not just for explicit threats. Reputation can lead to threats.
    b. Diverse social media monitoring. Social media is proliferating significantly, and security teams need to monitor as much as possible with the time and resources available. This means monitoring not just established social media but rising ones as well.
    c. Develop an understanding of how your brand sits within the main and emerging political discourses, extremist ideologies, and conspiracy theories.

If your business would like to understand any of these issues more deeply, you can find us at insightforward.co.uk or contact us directly.

Insight Forward provides a range of intelligence services to help businesses stay secure and thrive in an increasingly complex global marketplace.

Intelligence Analysis
We specialize in corporate intelligence. With a deep understanding of geopolitical trends, regional dynamics, and security issues, our services provide comprehensive intelligence reports and insights to support informed decision-making for businesses.

Consulting
Whether you're building a team or evaluating your team's capabilities, our tailored intelligence solutions offer valuable assistance. We understand the unique requirements of corporate intelligence programs and provide comprehensive support to help you achieve your objectives.

Monitoring
Our regular monitoring services encompass tracking threats, assessing emerging risks, and offering forecasts on global developments, geopolitical trends, and security incidents.

Training
We offer a range of training services suitable for individuals aspiring to launch their career in corporate security intelligence, as well as experienced analysts seeking to refine their skills.