

# **The Growing Threat of Misinformation and Disinformation:** How to Defend Your Organization and its Reputation



---

## Introduction

Today's information environment is vast and complex. The internet has increased the dynamism and scale of information available to us in each moment and secured fundamental changes in how we seek out, acquire, and digest information. These changes have been accelerated by the online social networks and social media platforms that connect billions of users worldwide and enable individuals to instantaneously generate, share, and interact with information. This democratization of information sharing provides enormous opportunities, but it also gives rise to challenges and dangers on an extraordinary scale.

The ubiquity of social media, its accompanying ease of use, and simple functionality has propelled an increasing public reliance on these digital platforms for everyday information and news. According to Pew Research, in the United States alone, about two-thirds of the population at least occasionally get their news from social media.<sup>1</sup> Exposure to social media content then shapes, informs, changes, and reinforces individual beliefs, attitudes, and values, often confirming or entrenching past perceptions more deeply — for better or for worse.

Yet, much of the “news” captured on social media comes from indefinite, undefined, misrepresentative, or noncredible sources. In fact, 57% of those who often get their news from social media say they **expect** the news they see on these platforms to be in some way inaccurate. Unfortunately, it is unclear how these concerns are subsequently mitigated. In this way social media is a communications medium extremely susceptible to the threat and spread of both **disinformation**, defined as the dissemination of false information purposefully crafted to mislead others (often as active measures by our adversaries), and **misinformation**, which involves the spread of incorrect and misleading content, but without an intent to deceive. While a key distinction is the intention of the user disseminating the information, the impact of the malign information's spread can be equally destructive, whatever the original intent.

---

<sup>1</sup>Elisa Shearer and Katerina Eva Matsa, “News Use Across Social Media Platforms 2018,” *Pew Research Center*, September 10, 2018, <https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/>

## Origins

While the origins of disinformation and misleading propaganda stretch back through history, our modern understanding arguably has roots in the 20th Century. Notably, the CIA highlighted the potential for “Strategical Psychological Warfare” in 1949, establishing communications strategies and the ability of coordinated messaging to be an offensive weapon “knowing no limitations in time or space.” Moving from World War II into the Cold War era, an interagency committee established and executed U.S. policy to respond to the Soviet Union’s disinformation with strategic communications. Today, continuous advances in communications technology and an increasingly globalized information environment have cultivated real-time information flows in a novel digital battleground that require a vigilant, proactive approach.

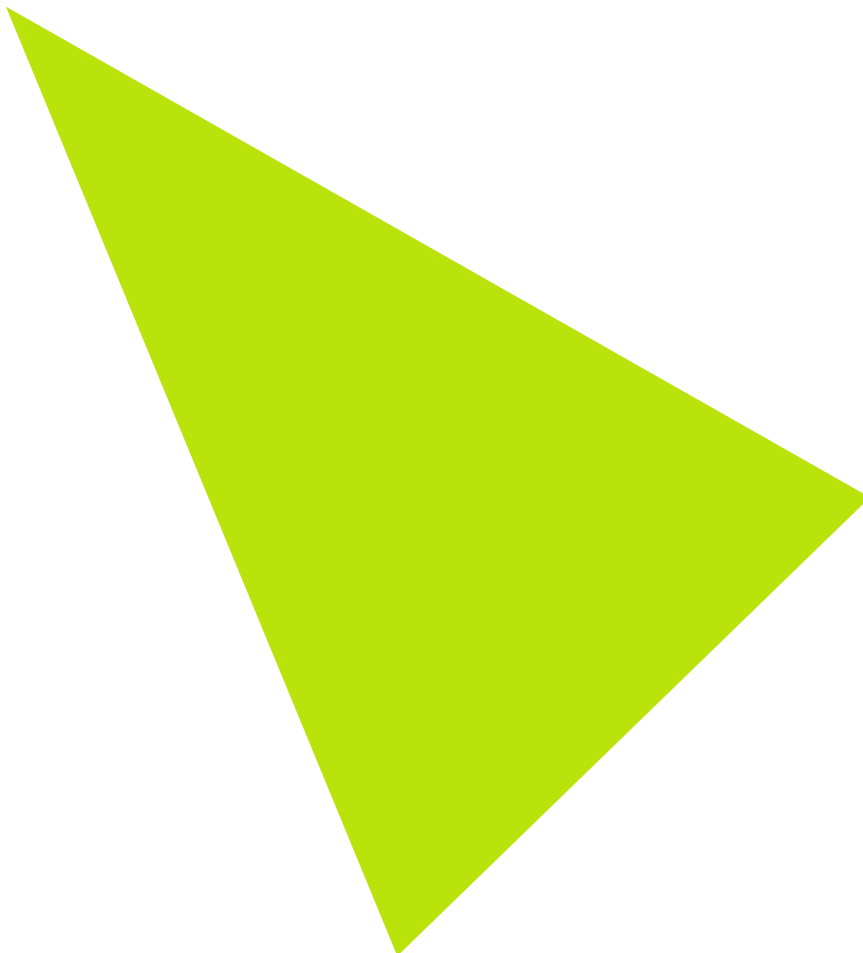
Consider the emergence and increase of deep fakes which exploit artificial intelligence to generate utterly realistic, but fabricated images and videos that depict false and doctored realities.

Increasing advancements in technology exacerbate today’s threat of misinformation and disinformation. Consider the emergence and increase of deep fakes which exploit artificial intelligence to generate utterly realistic, but fabricated images and videos that depict false and doctored realities. Social media platforms apply tailored and personalized algorithms that curate the information each individual user is exposed to, based largely on a user’s previous online behaviors and information selections. In this way, the algorithms themselves can be passively hijacked and weaponized to continuously spread false information. This curation of content compounds with social media’s enormous reach to expediently disseminate information on a global scale. Social media has created the experience of “viral” information circulation based on the sheer speed at which information can spread within and across platforms. The amplification effects this creates can have devastating consequences for the public at large when the viral information proves to be misleading, inaccurate, and/or intentionally deceiving.

While some companies that own prominent social media platforms, such as Facebook, Twitter, and YouTube, have “pledged” to more vigorously ferret out, remove, or otherwise flag potential disinformation or misinformation hosted on or disseminated through their sites, this self-policing of content and good-faith compliance can prove challenging for a host of reasons and, therefore, relying on these companies alone to identify and remove misinformation or disinformation — especially that which may be damaging to your organization — is not a realistic mitigation strategy.

For these reasons, it should come as no surprise that it is critical for leaders to understand and position their organization for the new “normal” of today’s information environment — one that accelerates the spread of misinformation and disinformation, and significantly broadens its potential reach and impact. It is no longer optional for good stewards and leaders to prepare, develop strategies, and formulate best practices to counteract false or misleading narratives that could damage an organization’s reputation, brand, and well-being. Rather, it is a vital imperative for them.

Leaders must proactively analyze and create strategies to confront a potential misinformation or disinformation incident or campaign. This can be achieved most successfully through powerful and unrelenting information monitoring, the engineering and implementation of a strategic communications strategy that acknowledges misinformation and disinformation, and keen preparedness to mitigate the harmful impacts of malign information when it surfaces.



## COVID-19 and Social Media

### A Case Study of Misinformation and Disinformation During a Deadly Crisis

The COVID-19 pandemic is a global crisis with devastating effects in terms of magnitude, human catastrophe, and disastrous economic dislocation. While many response efforts focus on arming the public with accurate information about the virus, misinformation about COVID-19 has proliferated dramatically and been equally infectious. This is true despite an aggressive effort by international bodies, national and local governments, and traditional and social media companies to prevent this dissemination of misinformation and disinformation. In fact, the spread of false information on COVID-19 has become so rampant and pervasive that the World Health Organization coined the term “infodemic” to describe the vast conspiracies, unsubstantiated claims, and apocryphal remedies surrounding the outbreak.<sup>2</sup>

For example, social media has also proven to be fertile ground for the spread of misinformation about the efficacy of various home remedies for combating the virus — from ingesting garlic or drinkable silver, consuming “miracle minerals,” concocting homemade hand sanitizer, drinking water every 15 minutes, or exposing oneself to excessive amounts of heat (via taking hot baths, drinking hot water, or using hair dryers in unconventional ways). All of these at-home theories have been summarily discredited by either the U.S. Food and Drug Administration, the U.S. Centers for Disease Control, the World Health Organization, or the United Nations Children’s Fund. Yet, the spread of these “remedies” as cures or proper preventive measures has nevertheless continued despite the pronounced and explicit dispelling of these remedies as appropriate.

---

<sup>2</sup> John Gregory, “The coronavirus ‘infodemic’ is real. We rated the websites responsible for it,” *NewsGuard*, February 28, 2020, <https://www.statnews.com/2020/02/28/websites-spreading-coronavirus-misinformation-infodemic/>.

---

## Guidehouse's Unique Approach to Misinformation and Disinformation Detection

In close coordination and collaboration with an organization's leaders, Guidehouse applies a six-step approach to misinformation and disinformation issues for our clients. This approach can be applied in the public or private sectors, and across industries and issue areas.

1

### **Understand the reputation, mission, and broad themes to be protected.**

This is the information that the dedicated misinformation and/or disinformation team will be chartered to protect. Critical to detecting malign anomalies or deviations is a foundational understanding and agreement on what needs to be protected.

2

### **Configure and deploy the tools and technologies that will be used to monitor the information landscape.**

Much like cybersecurity, detecting and responding to misinformation and disinformation effectively requires a customized approach based on the needs, requirements, and sensitivities of your organization. Configuring and deploying the right tools and technologies based on your organization's specific risk profile is critical to maximizing detection and mitigation efforts. It also enables our approach to stay agile, and incorporate new, emerging technologies as necessary. These include the data streams that the team will be monitoring (i.e., identifying sites that represent higher risk) — and the tools it will use — to search for, capture, and diagnose potential misinformation/disinformation.

3

### **Identify information that has deviated from accurate or intended messaging and analyze its informational attributes.**

Deviations from intended messaging or communications are normal and expected; however, they may also be an indicator of potential misinformation or disinformation. Our team identifies these deviations and evaluates how the identified information may be wrong, the background of the individual/organization posting or publishing the information, and whether the amount of deviation from the intended message warrants further action based on its effects or potential impact. Informational attributes assessed in this step include source type and integrity, readership or following size, user profile indicators, degree of messaging deviation, posting patterns and frequency, original content forensics, and signs of falsified or fabricated proof points (e.g., deep fakes or forgeries).

## Monitoring the Indexed and Unindexed Internet

In addition to monitoring traditional and social media platforms, Guidehouse can also employ its dark web monitoring capability as a part of its misinformation and disinformation services to collect, analyze, and visualize data from illicit forums, marketplaces, chat services, blogs, paste sites, card shops, and other sources. This deepens our team's ability to identify potential threats to — and vulnerabilities of — our clients, and to recommend earlier and/or more holistic actions to mitigate the risks and dangers.

Based on our experience, Guidehouse believes that dark web threat monitoring and subsequent mitigation actions are crucial to identifying threats and allowing for a coordinated response before relatively small schemes spill over into the traditional and wider social media conversation where they can instantly generate negative impacts that require full-blown crisis communications and campaign optimization activities, such as the deployment or relocation of paid media resources.

4

### Assess risk and continuously monitor the information spread.

This step is the first in a sequence of translating misinformation or disinformation discovered through continuous monitoring and analysis into a course of action or recommended intervention. Our team maps the informational attributes to a risk matrix and presents the key, fact-based findings, along with supporting documentation. Critically, this step places the analysis within a risk assessment framework and applies weights to the information's likelihood for damage so that findings can be prioritized for action.

5

### Develop counter-messages to inaccurate or false information.

When identified misinformation or disinformation moves into this stage, it's time to act. This often involves contacting and engaging key partners — social media platforms, traditional media outlets, the sources of misinformation and/disinformation themselves, online search engines, and allies and partners — that play a role in the dissemination and sometimes countering of information. It also involves engaging key partners within your organization's leadership, risk management, and communications teams to develop and implement a counter-messaging plan built on fact-based, data-driven research, and audience resonance. Implementation of the plan may also involve coordinating dissemination of the counter-message with partners or other key stakeholders who are viewed as less biased respondents to the malign information.

6

### Evaluate the efficacy of the counter-messaging.

Once a counter-messaging strategy has been developed and executed, the team will monitor the response to and impact of the counter-message within the information environment so that measures of effectiveness can be assessed, and activities can be adjusted and executed accordingly. This qualitative approach allows deployment of continuous monitoring and countermeasures, creating an agile feedback loop that can adjust to constant changes within the social media landscape in real time.



---

## How Can Guidehouse's Misinformation and Disinformation Capability Benefit Your Organization?

Within Guidehouse, we have the tools, automation, technology, methodology, framework, expertise, and experience to identify, evaluate, mitigate, and deter misinformation and disinformation affecting our clients, and we guide our clients on how best to respond. We offer the following services to organizations, officials at the federal, state, and local levels, nonprofits, and private individuals:



### **Risk assessment:**

Evaluate whether misinformation and/or disinformation is an issue for your business or mission and — if so — how significant it is, how it is happening, and how successful mitigation measures deployed thus far to address it have been.



### **Threat and risk identification and monitoring:**

Monitor social media and digital sources for misinformation and/or disinformation about your organization, office, program, or mission area. This service identifies and assesses information threats across an array of defined risk categories.



### **Threat sharing:**

Coordinate the sharing and reporting of misinformation and disinformation with partners, agencies, technology companies, and key stakeholders as appropriate, using the most effective channels and following the necessary protocols.



### **Defense and response:**

Develop tactical response and mitigation plans that include processes for potentially alerting law enforcement to instances of disinformation; reporting misinformation and disinformation to social media platforms for removal or warning; and possibly leveraging social media's broad reach to raise public awareness of disinformation in particular, so that attempts to suppress or dissuade voting, for example, can be neutralized. Services like these extend far beyond social media monitoring — they translate the power of social media into tangible, high-impact action and responses.





### **Crisis communications and management:**

Provide triage support to a government agency, company, or individual affected by either misinformation or disinformation. The development of effective communications strategies is a critical element of crisis management.



### **Education and training:**

Provide misinformation and disinformation education to an organization and its representatives to increase and enhance awareness around the issue. This includes training your team on key indicators; useful tools to discover, identify, and attribute (where possible) misinformation and disinformation propagation; and techniques for fostering preparedness.



### **Advisory services:**

Develop a misinformation and disinformation strategy that fosters a communications culture of safeguarding your organization and its reputation against the potential impact of malign information. Provide guidance on establishing a multifaceted approach to mitigating the effects of misinformation and disinformation.

## **Guidehouse's Solution in Action – Defending Against Misinformation and Disinformation**

---

Guidehouse is currently playing a critical role in protecting the integrity of the 2020 Census by identifying, analyzing, and mitigating the impact of misinformation and disinformation that interferes with the Census Bureau's constitutional mandate to count all persons in the United States and its territories. Guidehouse supports the execution of this mission through effectively monitoring social and traditional media platforms, supporting the development and dissemination of accurate and informative counter-messaging as necessary, and engaging with key stakeholders to coordinate response. Guidehouse also works with multicultural communications experts to assess emerging issues and threats specific to diverse communities and engages with traditional media outlets and trusted voices in those communities to dispel rumors and disinformation.

Two threats that were mitigated before they could develop into potential crisis situations include:

### **A false rumor that Census teams were canvassing communities which increased the risk of burglaries.**

This hoax derived from malign information in South Africa and was successfully identified by the team and removed from multiple platforms. This rumor eventually resulted in a formal response from the Census Bureau.

### **Inaccurate perceptions that Census completion was tied to the COVID-19 stimulus.**

Addressing and countering the false statements — which appeared across platforms and in multiple posts — required coordination between technology partners, fact-checkers, and civil society partners. Ultimately this discovery also resulted in a formal response from the Census Bureau and a page on PolitiFact.

---

## Why Guidehouse


Guidehouse delivers actionable solutions that allow our clients to meet and defeat threats in real time. Our focus on quality through execution brings forth the best and brightest minds to support projects that drive meaningful change. This, in turn, fosters insight and innovation to meet mission objectives based on the ever-changing threat landscape. Our clients rely on Guidehouse not only because we provide strategic and operational recommendations based on reliable, real-time data, but also because our guidance leads to informed decision-making, action, and high-impact solutions.

Guidehouse provides best-in-class capabilities to organizations seeking to combat misinformation and disinformation and integrating advanced technology with the expertise of subject matter experts and technical experts to detect misinformation and malign actors. We work with our clients to detect, deter, and defend against these misinformation and disinformation efforts by designing and executing operational strategies to defeat them. The Guidehouse team leverages a full spectrum of sources — social media platforms, online forums, blogs, company records, government databases, proprietary internal Guidehouse databases, global business electronic filings and databases, and the dark web — allowing the team to create a common operating picture of potential risks and to monitor them accordingly. The Guidehouse team is continually evaluating and adding new technology, tools, and sources based on the needs of our clients, and our team has the flexibility to incorporate custom sources as needed for specific and often sensitive projects.



**Email:** [opensource@guidehouse.com](mailto:opensource@guidehouse.com)

**Web:** [guidehouse.com](https://guidehouse.com)

 [@guidehouse](https://twitter.com/guidehouse)

 [linkedin.com/company/guidehouse/](https://linkedin.com/company/guidehouse/)

© 2020 Guidehouse Inc. All rights reserved. This content is for general informational purposes only, and should not be used as a substitute for consultation with professional advisors. This publication may be used only as expressly permitted by license from Guidehouse and may not be otherwise reproduced, modified, distributed, or used without the expressed written permission of Guidehouse. GH-108a WP