The Do Something Doctrine: A Corporate Guide to Counter-Disinformation

By Colin P. Clarke and Zach Schwitzky

Introduction

In today's information environment, multinational corporations face unprecedented risk, compounded by extreme geopolitical volatility, rapidly emerging technologies, and a lowering of the barriers to entry for the wide range of entities peddling disinformation. In 2024, conflicts continue to rage in the Middle East and Ukraine, tensions abound in the Indo-Pacific region, and the U.S.-Mexico border remains a major flashpoint, providing nefarious actors with ample opportunities to push a litany of false narratives. In a survey from the World Economic Forum on the risks most likely to trigger a global crisis over the next two years, misinformation and disinformation ranked second.

In July, the Paris 2024 Summer Olympics will kick off, with organizers anxious about a range of potential disinformation-related issues that could affect the games and its corporate sponsors. Globally, more than 4 billion people are registered to vote in the most significant election year in history, increasing the likelihood of foreign information manipulation and interference. Partisanship and extreme polarization overlap with identity politics and generational mistrust of institutions and news media to exacerbate societal strife. The misuse of artificial intelligence for malign purposes, including so-called 'Deep Fakes,' remains a concern.

There were similar issues in the lead-up to the 2016 and 2020 U.S. Presidential elections. Following these pivotal moments, many so-called "counter disinformation" companies proliferated, flooding the market and jostling for position to offer services as the public and private sectors attempted to navigate a critical paradigm shift. However, as newly formed companies scrambled to corner the "counter-disinfo" market–offering a host of proposed solutions – from bot detection to narrative and network analysis – it fed a nascent "Disinformation Industrial Complex." Seemingly overnight, a cottage industry sprouted up, promising to abate the asymmetry between fact and fiction. Accordingly, it became more difficult to discern meaningful differences between these companies and their respective offerings.

Led by Western democracies, there has been a sea change in the strategies for dealing with disinformation. A general shift is underway from monitoring the information environment to identifying risk to developing operational capabilities to counter foreign information

manipulation and interference. Much of the research and government-civil society collaboration focuses on understanding malicious actors and categorizing influence operations. And, despite their claims, most companies operating in the "counter-disinfo" space offer glorified monitoring capabilities. Organizations operating in today's information environment require a practical, response-focused solution to evaluate risk, build resilience, and mitigate crises.

Most of the services and capabilities these "counter-disinfo" companies offer are best termed "upstream" capabilities, suitable for some (primarily governments) but providing few tangible benefits to an organization looking to build resilience and effectively mitigate a crisis. As more "counter-disinfo" companies secure funding from venture capitalists, there is growing pressure for them to prioritize expansion over function. The private sector presents growth opportunities, especially with an uneducated buyer. Corporate executives have a responsibility to shareholders and stakeholders and need to understand the difference between disruption (upstream) and mitigation (downstream) and which "counter-disinfo" providers offer worthwhile solutions.

Below is a guide to "counter-disinfo" services and providers for corporate executives, providing answers to frequently asked questions…

What tools and skill sets do organizations need to operate effectively in the modern information environment?

To be optimally positioned to succeed in the modern information environment, organizations require a three-pillared approach: (1) utilize innovative technology able to accurately assess the potential impact of an emergent situation, especially a crisis; (2) communications expertise, so if a response is required, seasoned communicators can guide the response; and (3) subject matter expertise on geopolitics and international relations (the "human in the loop"), to help navigate the complex global environment that shows few signs of stabilizing any time soon.

The trust and safety of the information environment is a constant issue. What steps can an organization take to make progress in this area?

Establishing trust and safety in the information environment requires a whole-of-society response. While this phrase is somewhat trite and perhaps cliché, it means governments, tech platforms, civil society, academia, multinational companies, and individuals each playing a role in the information environment. Broadly, these responsibilities can be categorized as follows:

- **Education**: Teaching digital and media literacy remains a generational challenge but can broadly impact the effectiveness of fake news and other malign online activities, as evidenced in Finland and other Nordic countries. Investing in education and prevention is costly and can take time to demonstrate results, which is why it remains politically unpopular, but public-private partnerships may be one way to alleviate this burden.

- **Policy**: Both federal and local regulation and the implementation of effective trust and safety policies at tech platforms can make it more complex and more expensive for malicious actors. This issue was brought to the forefront during the COVID-19 pandemic with the proliferation of the QAnon conspiracy theory.

- **Litigation and Sanctions**: Criminal charges, civil lawsuits, and sanctions are designed to disrupt malicious actors. Over 1,900 individuals and entities have been sanctioned in Russia, while more than 24 billion Euros of private assets in the European Union (EU) have been frozen.

- **Technical Response**: Offensive cyber-attacks and platform takedowns make it more difficult and expensive for malicious actors to operate. However, each platform takes a slightly different approach, and guidelines can change, as has occurred with some tech platforms that are now far more permissive in allowing malign activities to proliferate.

- **Exposure**: Journalists, academics, and civil society have effectively exposed the individuals and entities behind malicious networks and campaigns. More funding devoted to investigative journalism and research is a global public good and will directly impact analysts' ability to cover disinformation and influence operations.

- **Resilience Building**: Educating your employees, customers, and other stakeholders remains crucial. Part of this is defining and communicating your organization's values and ensuring they resonate with the workforce. Another critical piece of resilience is understanding your acceptable level of risk and engaging with effective counter-disinfo technology solutions and partners.

- **Countermeasures**: These can encompass a broad range of actions, including responding to or fact-checking a false narrative, providing alternative information to key stakeholders, working with journalists, partners, or a trusted network to convey the organization's position on a particular issue or situation. However, the risk of disinformation is never static, and countermeasures cannot be either, thus necessitating constant monitoring of new trends in disinformation and innovative solutions to meet challenges as they evolve and morph over time.

Are disruption and mitigation the same thing?

The first five of the tactics detailed above are "upstream" solutions. In other words, these remedies are either intended to disrupt malicious actors and/or inoculate the population from disinformation and false narratives. While there is not necessarily a shared model to analyze and disrupt threat actors and the tactics of malicious influence operations, investigators from

government, civil society, academia, and the private sector often refer to a kill chain, which allows them to gather and compare insights into operations and increase the chances of disrupting malicious actors. The only genuine "downstream" mitigation options are resilience building and countermeasures.

Since disrupting the threat does not mean it is entirely extirpated, the effectiveness of the disruption effort is short-lived. The threat will metastasize again quickly, forming new networks and workarounds. In short, there will always be a baseline level of risk for organizations operating in the information environment, which inevitably necessitates a comprehensive and downstream response.

In the moment of crisis, what are the right questions to ask?

In a moment of crisis, many organizations find themselves in an uncomfortable predicament– ill-prepared and uninformed. For example, when Hamas launched a terrorist attack against Israel on October 7, 2023, few multinational corporations saw risk to their own businesses. Yet, just weeks into the conflict, some of the most recognizable brands in the world found themselves facing boycotts–McDonald's, KFC, Burger King, Pizza Hut, Starbucks, and Coca-Cola, to name just a few. Yet what do any of these brands have to do with terrorism and war in the Middle East? As an executive at one of these companies, you may run through a short list of questions:

- *What do we believe is an acceptable level of risk?*
- *Do we have a specific position on the issue or situation?*
- *What are the possible response options?*
- *What is the cost of doing nothing?*

Ideally, the general responses to these questions are tailored to the organization well in advance of a crisis, on the shelf and readily operationalized. With some introspection, planning, and proper resourcing, organizations can be well-positioned to weather emerging risks.

Does narrative analysis, bot detection, or content authenticity matter in a moment of crisis?

The gravest risk of contracting with certain companies offering "counter-disinfo" services or technologies is paying to become misinformed. Narrative analysis, network analysis, bot detection, detecting inauthentic content/activity, and related actions can help support disruption efforts. But the outputs of these glorified social listening tools and OSINT-adjacent capabilities masquerading as artificial intelligence (AI) merely provide possible evidence for policymakers, law enforcement officials, lawyers, and trust and safety teams at tech platforms, who might utilize this data to levy sanctions, file civil or criminal charges, or remove accounts and/or content. None of these outcomes help an organization in a moment of crisis. Even in an ideal

scenario, the most immediate result of these "upstream" capabilities is de-platforming. Still, there are second-and third-order effects to consider, including that removing accounts may simply cause the threat actor(s) to target the brand with more vengeance, with different accounts and tactics making the previous expensive and time-consuming evidence-gathering efforts futile.

The reality is that worrying about whether fake accounts proliferate a coordinated attack against your brand misses a critical point – what is the potential impact on my business, and what is the appropriate response? As generative AI has demonstrated in recent months, synthetic content is just as believable as organic content in many instances. Corporate executives are responsible to shareholders and stakeholders tasked with protecting the bottom line. Paying for "upstream" capabilities is the non-tax beneficial equivalent to donating to the Center for Countering Online Hate or other nonprofits working to make the internet a safer place.

Ask yourself, in a moment of crisis, does it truly matter if the activity is inauthentic or organic, if it's negatively impacting my business?

Falling victim to the 'do something doctrine' is easy because 'doing something' makes you feel active, and active feels effective; it's better than nothing. But is it right? The critical question is not, "What should I do?" but rather, "If I decide to act, how will that impact my business?"

How should we evaluate "counter-disinfo" companies?

Companies that promise to counter disinformation, uncover threats, or identify media manipulation are too often unequipped with the proper tools to effectively assess the risk elements in today's information environment that should most concern private industry. Identifying fake accounts and bots, mapping the spread of disinformation, and visualizing link analysis may provide situational upstream value or evidence. Sentiment analysis is more generic and typically available with other widely used social listening tools. And real-time alerts can do more harm than good, creating a situation we call "Henny-Penny" syndrome, as with every real-time alert, it seems as if "the sky is falling." Real-time alerts on fake accounts and bots can be more akin to fear-mongering, mainly when they include information that is not actionable for an organization and may only result in punitive measures against malicious actors at some point down the road.

When a crisis hits, would you rather be uninformed or misled? Do you follow your gut instinct to react, firing off a series of tweets to show you are engaged, or do you eschew a response, gather more information, and then decide whether to issue a formal statement? In the midst of a crisis, there is typically a sense of urgency to *do something,* but what does that something look like, and is it informed and well-timed? In many situations, the most effective response is no response at all.

Without the ability to determine the potential impact of risk in the information environment, even the most well-intentioned counter-disinformation services or technologies will fail. In some cases, they can be counterproductive, exacerbating underlying issues and worsening the problem.

Do we need anything more than our existing social listening provider?

If you currently pay for a social listening service, you'll likely pick up on most narratives as they explicitly mention the company, a product, or an executive. The need, then, is to understand the potential impact of these narratives. Most counter-disinfo services offering their version of narrative analysis will analyze where a narrative originated, how it spread, and the overall sentiment. Still, these do not tell you if and how it could impact your business and what you should do about it.

In a moment of crisis, there is only a nominal case to be made for the value of understanding inauthentic activity, foreign amplification, or the campaign's origins. These steps can help tech platforms consider account or content take-downs. They can also inform responses in the event of state-backed activity targeting your organization, like H&M, in early 2021 after the company decided to stop sourcing cotton from Xinjiang. But these "upstream" actions do little for a private sector entity in a moment of crisis. Cross-platform analysis can be potentially beneficial, but only if a threshold of acceptable risk has been defined and a mechanism established to quickly determine whether that threshold has been exceeded.

Most counter-disinfo companies aggregate data from sources similar to popular social listening services, like Netbase Quid, Brandwatch, Sprinklr, and Meltwater. Whether positioned as threat intelligence or narrative intelligence, err on the side of parsimony when paying for multiple vendors providing redundant capabilities, despite how these vendors may claim to leverage AI.

In short, many "counter-disinfo" companies will attempt to sell their own version of a social listening tool. Yet, oftentimes, this is a capability most organizations are already paying for in the first place. Simple queries in an existing social listening tool will identify most of the same brand-specific narratives these counter-disinfo companies are picking up.

Social listening tools can even be counterproductive, especially when viewed as a panacea. They offer a false sense of security to an organization that believes it is getting far more than is offered. In times of crisis, what seems like a minor capability gap can morph into a glaring vulnerability, with devastating consequences if handled poorly.

What is narrative intelligence, and do we need it?

This capability includes a range of techniques, including surfacing emerging narratives, cross-platform or multichannel analysis to identify disinformation and social media manipulation, and network analysis to map the origin and spread of online narratives. Many organizations already

have robust social listening capabilities. Simple Boolean queries and topic modeling in most social listening platforms will enable you to identify narratives about your company, products, and people.

What is threat intelligence, and do we need it?

Threat should refer to the wide range of malicious actors attempting to leverage disinformation to cause financial, reputational, or other harm. But threat is often conflated with risk; people naturally relate to the idea that something is being done to them (threat) more so than something is happening that could impact them (risk). Companies offering threat intelligence attempt to address actor capability and intent with services like bot detection, identifying fake accounts, attribution to foreign actors, and content evaluation tied to toxicity, polarization, or even truth and fiction.

This capability is only useful on a cursory basis. In certain situations, your response may radically differ if a state-backed influence operation targets your organization. Beyond that, these capabilities should be reserved for OSINT analysts gathering evidence for government agencies, law enforcement, and tech platforms.

Is it helpful to be alerted to deep fakes?

In short, no. Like inauthentic activity, alerting to the existence of deep fake or other synthetic content misses a critical point—what is the potential impact on my business, and what is the appropriate response? Synthetic content has proliferated online, but much of it is not malicious. Accordingly, it is even more critical to understand the potential impact of a narrative or campaign targeting your organization, regardless of whether the content is authentic and the activity is organic.

Do we need a solution to evaluate risk in the information environment?

This is not real-time fact-checking. Instead, this capability should proactively evaluate a narrative's potential spread and resonance. The ability to quickly assess the potential impact of an online narrative or other information that could negatively impact your organization is critical. Whether you decide to layer this capability on top of your existing social listening tool or engage with a provider offering a dedicated risk assessment solution, quickly evaluating a narrative's potential impact is crucial. Effective risk assessment includes not just engagement-driven metrics, which are relatively easy to quantify and predict, but an emotive indicator like belief, resonance, or impact.

Do we need crisis communications?

This function will help you build resilience and evaluate and execute possible response options during a crisis. Comprehensive reputation and crisis management focuses on building resilience,

responding effectively, and operating in an environment of often intense scrutiny. Most organizations are not yet equipped to navigate this type of crisis in-house, so having access to seasoned crisis communications professionals is vital. In a moment of crisis, you want a trusted partner to help you protect or restore your reputation and regain the confidence of the people who depend on you.

Do we need geopolitical subject matter expertise?

These practitioners continuously monitor and analyze situations on and offline to identify threats percolating below the surface and how they could impact the private sector. Subject matter expertise should focus on geopolitics, international relations, and the information environment to help you operate in high-risk, high-opportunity environments.

If you're being targeted for your position on the Israel-Hamas conflict, you need access to a leading subject matter expert, not someone who scrolls X (Twitter) for a couple of hours and lacks the experience and training to understand complex geopolitical dynamics with decades-old roots. Given the volatility of today's information environment and simmering global tensions, this function is critical for effective resilience building and crisis management.

Are there real-world examples?

What do a fast-food chain and a beer brand have to do with modern-day conflict? On the face of things, nothing at all. But in today's complex information environment, no company or brand is immune from the volatility of geopolitics. Any organization can become the target of a disinformation campaign, and the reasons driving these attacks can vary widely. However, corporate executives can make the choice to build resilience and implement countermeasures to mitigate the negative effects of disinformation campaigns and the viral spread of false narratives about their businesses.

McDonald's

When the conflict in Gaza first erupted in October 2023, McDonald's soon found itself in the crosshairs of protesters and demonstrators calling for a global boycott of the company after locations in Israel allegedly gave free meals to Israeli soldiers. Chief executive Chris Kempczinski condemned "violence" and "hate speech" and said all franchises in Muslim countries are owned by "local owner-operators who work tirelessly to serve their communities while employing thousands of their fellow citizens."

These calls for boycotts fueled demonstrations in countries including Australia, Indonesia, the United Kingdom, and the United States. Many of these protests included acts of vandalism and the destruction of property, which intimidated customers and kept people from patronizing the restaurant. Some of these protests were also linked to the wider Boycott, Divestment, and

Sanctions (BDS) movement, which calls to put pressure on Israel to change its policies in the Palestinian territories. On March 22, 2024, McDonald's Malaysia dropped its lawsuit against the local chapter of the BDS movement.

On its social media accounts, McDonald's Israel promoted its donation of thousands of free meals to Israeli Defense Forces personnel. The accounts later stated that the franchise was donating meals "to all those who are involved in the defense of the state, hospitals, and surrounding areas." Franchises in Muslim-majority countries, including Saudi Arabia, Oman, Kuwait, the United Arab Emirates, Jordan, and Turkey, issued statements disavowing the move.

Unlike Starbucks, which was assailed as pro-Palestinian in North America, while in the Middle East and Muslim-majority countries in Southeast Asia, including Malaysia and Indonesia, the company was accused of being too pro-Israel. Calls to boycott McDonald's were almost entirely driven by the company's supposed pro-Israel stance. Kempczinski admitted the boycotts are "hurting business," claiming the company is seeing a "meaningful business impact" due to "misinformation" about its position in the Israel-Hamas war.

While there are nuances and challenges with McDonald's local owner-operator business model, Kempczinski's January 4, 2024, LinkedIn post did little to quell the protests or mitigate the resulting financial impact on the business. In his condemnation of "violence" and "hate speech," Kempczinski did not express support for Israel. Nor has the company issued any statements of support for Israel or the ongoing war in Gaza.

What is clear from McDonald's response is that, back in January, the company clearly lacked visibility on the global nature of the BDS movement and awareness of the underlying issue, blaming "misinformation" for hurting its business in the Middle East and other regions. Whether the accusations of the company's stance on the Israel-Hamas war were factually correct, the narratives resonated with global consumers. Spotting misinformation or determining the authenticity of related online activity would have been of little value to McDonald's; the impact was tangible and quantifiable.

Key Learning Outcome: *When it comes to response options, there is no one-size-fits-all approach. But there is not always a correlation between a narrative's veracity and its impact. Being able to quickly and accurately assess the potential impact of an emergent situation, access subject matter expertise on geopolitics and international relations, and leverage seasoned communicators with on-the-ground cultural experience is critical in the moment of crisis.*

Heineken

Heineken, the global beer brand based in the Netherlands, found itself in the unenviable position of being listed in July 2023 on Yale Professor Jeffrey Sonnenfeld's compendium of countries

continuing to do business in Russia. The following month, in August 2023, Heineken sold its operations in Russia for 1 Euro, resulting in a 300 million Euro loss.

Heineken was criticized heavily for promising to leave Russia shortly after its brutal invasion of Ukraine in February 2022. However, the company delayed its exit, perhaps believing the war might end quickly, obviating the pressure to shut down its operations. Whatever calculations the leadership at Heineken made about the duration of the Ukraine war, they were wrong. The mixed messages and feet-dragging were made worse by revelations that not only did Heineken remain in Russia long after it promised to withdraw, but that it actually expanded its operations, attempting to snap up market share from other beer brands that did leave the country.

In a fairly obvious statement that poorly reflected Heineken's leadership, CEO Dolf Van den Brink said, "Recent developments demonstrate the significant challenges faced by large manufacturing companies in exiting Russia. Heineken's experience is an example of the worst of both worlds–being assailed for remaining in Russia, thus damaging its brand reputationally, ultimately withdrawing due to building pressure, and suffering a drastic financial loss in the process. Poor communications, indecisiveness, and a clear lack of understanding of the geopolitical context led to an unnecessary black eye for a company that should know better.

Key Learning Outcome*: By initially proclaiming its intention to close operations in Russia, to much acclaim, Heineken hesitated, delayed, and ultimately remained in the country until the pressure became untenable. So, in the end, Heineken suffered massive financial losses, and its brand and reputation were besmirched. The company failed in its strategic communication efforts and failed to assess the backlash from being associated with Russia. With geopolitical expertise, Heineken executives may have become more aware of the brutality of Vladimir Putin's actions in Ukraine and the severity of global public opinion against Russia. In parallel with seasoned communicators who use a data-driven approach, Heineken could have reached a different decision and thus avoided significant financial losses.*

Conclusion

As modern disinformation rightly becomes an area of concern and focus, companies offering "counter-disinfo" services are often misaligned to the nature of the threat (especially in the midst of a crisis), leaving corporate executives lacking necessary real-time insights and advice on whether or not to act and how. Put bluntly, not all "counter-disinfo" services are created equal, and many of the "upstream" services offered will be little or no help in responding to a crisis like the war in Gaza. The differences between upstream and downstream capabilities and the importance of focusing on specific downstream capabilities, such as resilience building and various countermeasures, can mean the difference in effective mitigation.

To correctly manage risk in the information environment, corporate executives would be well-suited to pursue a three-pillared approach that provides innovative technology able to accurately assess the potential impact of an emergent situation, especially a crisis; communications expertise, so if a response is required, seasoned communicators can guide the response; and subject matter expertise on geopolitics. As the above case studies demonstrate, there is a pressing need to harness a suite of capabilities to combat disinformation, particularly amid ongoing global conflict and crisis. Having access to the right technology solutions and communications partner can help mitigate what could otherwise be a disastrous experience in dealing with the ubiquitous threat of disinformation.

Colin P. Clarke is a Senior Research Fellow at The Soufan Center and the Director of Research at The Soufan Group. He is also an Associate Fellow at the International Centre for Counter-Terrorism (ICCT) and a non-resident Senior Fellow at the Foreign Policy Research Institute.

Zach Schwitzky is the Co-Founder and CEO at Limbik, a cognitive AI company and a Mis-, Dis-, and Mal-information (MDM) Subject Matter Expert for the Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.