Teneo

From the Ballot to the Boardroom:
Lessons Learned from Election Disinformation Efforts

Teneo Insights | Election 2024

September 2024

Election-related disinformation campaigns have become a staple of modern election cycles, both in the U.S. and globally. Whether driven by foreign influence operations or domestic political or extremist groups, disinformation efforts are now an election mainstay.

While the effect of disinformation efforts on voters is difficult to assess, trends reveal how tactics leveraged in recent campaigns – from polarizing false narratives on mainstream and fringe social media platforms to coordinated bot attacks and deepfake videos – can be used to target organizations, brands and leaders long after the polls close.

Disinformation can be a powerful weapon to undermine trust, painting organizations and executives as politically compromised or unethical. False narratives can not only tarnish reputations, but also spark protests, civil unrest and cyberattacks, exposing organizations to real security risks. This analysis identifies five key disinformation trends to watch, along with strategies for staying ahead of these growing threats and related developments in the lead-up to the November 5 U.S. elections and beyond.

1. Social Media Influence Operations to Exploit Internal and External Divisions

The emergence of fake political groups on popular social media platforms exemplifies how disinformation campaigns in the form of social media influence operations can be designed to fragment political or ideological groups, or be leveraged for specific gains.

For corporations and other organizations, the implications are profound. Such influence operations can be developed by a variety of actors and stakeholders across social media platforms to exploit internal divisions within a company or between a company and its stakeholders. These operations have the potential to drive wedges between leadership and employees, or between a brand and its consumer base, by capitalizing on misleading information that can exploit and intensify existing tensions.

2. Disinformation Exacerbating Divisive Issues

Similarly, disinformation campaigns often exploit divisive social issues to exacerbate societal tensions. In this U.S. election season thus far, disinformation campaigns have targeted issues related to reproductive health, immigration, border security and U.S. support for Israel related to the current war in Gaza, seeking to further polarize the electorate.

Similar disinformation tactics can be readily utilized for the corporate context. An example is corporate Diversity, Equity and Inclusion (DEI) initiatives. Corporations that champion DEI programs could become targets of disinformation designed to polarize public opinion by falsely portraying these efforts as politically motivated or socially divisive. A company's DEI initiatives might be maliciously depicted as discriminatory against certain groups or as advancing controversial agendas, leading to public backlash, boycotts or internal discord, all of which can impact an organization's brand and reputation.

3. Deploying Generative AI Tools to Spread Disinformation

Generative AI-powered tools are increasingly being harnessed to generate and disseminate disinformation at-scale, with sophisticated algorithms enabling the creation of highly convincing fake news articles and deepfake videos and images.

Beyond election season, the takeaway is clear: generative AI tools can exponentially increase the reach and impact of disinformation, making it more challenging to detect and counteract misleading or inaccurate narratives in the digital domain. AI-generated content, the quality of which is improving at a rapid speed, has the potential to go viral quickly, undermining an organization's credibility and distorting public perception.

Not only can generative AI tools be leveraged for intentional disinformation purposes, but there is also the risk of inadvertent misinformation propagating. Automated social media posts or marketing materials generated by AI might include inaccurate or misleading information if not carefully reviewed. The cautionary tale for organizations is to balance the risks, along with the opportunities, when integrating generative AI into workflows, ensuring that all AI-generated content is rigorously vetted for accuracy.

4. Reductions in Online Content Moderation

Recent reports of social media companies scaling back their Trust and Safety teams or content moderation capabilities raise concerns about the long-term risks of disinformation spreading unchecked on these platforms. For instance, Meta's discontinuation of CrowdTangle, a tool used to track the spread of content across social media[1], limits the ability to monitor the dissemination of disinformation or coordinated campaigns targeting corporations.

This development underscores the need for heightened vigilance in detecting and countering disinformation in the digital landscape, particularly in terms of assessing the spread of negative content or narratives about an organization, the involvement of known disinformation networks and the amplification of content by suspicious or newly created accounts.

5. Disinformation-driven Violence

Finally, disinformation has the potential to incite physical violence. As we near election day in the U.S., high-profile polling locations or government buildings and landmarks, particularly in battleground states, could become flashpoints for protests, voter intimidation or witness the targeting of election officials and judges. Such activity would likely be driven by election-related mis- or disinformation. The convergence of opposing groups at locations like polling stations on election day increases the risk of potential clashes, which, in turn, could disrupt the voting process and create a potentially chaotic environment, especially if results are close or disputed or if there are delays in counting votes.

Recent riots in Southport, UK, triggered by false information related to the perpetrator of a horrific attack involving children[2], further demonstrates this risk. While this incident was not election-related, it demonstrates the dual risk of disinformation for corporations to consider. Not only does disinformation have the potential to impact an organization's reputation, but it can also lead to physical security risks for their

[1] Meta kills off CrowdTangle despite pleas from researchers, journalists | AP News

[2] Misinformation fuels tension over UK stabbing attack that killed 3 children | AP News

operations and employees. The Southport incident also highlights the importance of proactive crisis management and the need for robust security measures to protect against potential violence.

What Should Companies Do?

To effectively counter the growing threat of disinformation campaigns, Teneo's Risk Advisory team recommends organizations adopt a proactive and multi-layered approach. By anticipating potential vulnerabilities and preparing for a variety of scenarios, organizations can better protect their reputations, personnel and operations.

Below are key strategies that companies should consider implementing to stay ahead of disinformation campaigns.

- **Conduct Stakeholder Analysis**: Teneo's Risk Advisory team recommends organizations regularly conduct stakeholder analysis to understand the motivations and concerns of key groups; including employees, customers, investors and the broader public. Understanding these dynamics can help in identifying potential vulnerabilities that disinformation campaigns might exploit.
- **Engage in Scenario Planning**: We further recommend organizations develop and rehearse scenarios in which the company is targeted by disinformation campaigns, which allows for a proactive approach to threat management. This planning should include identifying likely vectors of attack, potential impacts and response strategies.
- **Implement Proactive Communications Strategies:** To get ahead of the variety of disinformation campaigns that may target an organization and its personnel or brand, Teneo's Risk Advisory team recommends that organizations establish clear, proactive communication strategies that articulate the organization's values and positions on key issues, thereby reducing the likelihood of disinformation gaining traction. For example, clearly communicating the intent and benefits of company policies and stances, while actively monitoring for disinformation targeting these initiatives, can mitigate damage and prevent misinformation from spreading further.
- **Develop Responsible Technology Practices**: As generative AI becomes more integrated into business operations, we recommend organizations adopt robust and responsible technology practices that include considering the ways that misinformation can be inadvertently propagated. This includes

implementing rigorous review processes for AI-generated content and continuously monitoring its impact.

- **Enhance Digital Intelligence Monitoring and Analysis**: The pervasive nature of disinformation campaigns underscores the necessity for organizations to proactively monitor inaccurate and adverse content to protect their key assets and reputation. Teneo's Risk Advisory team recommends organizations invest in robust digital monitoring tools and processes to proactively monitor narratives on mainstream and fringe social media platforms, identifying potential disinformation narratives and threats early. We recommend this include monitoring, not only for direct threats, but also for broader narratives that could impact the company indirectly. For example, indicators to watch include; the rapid spread of content that appears to pit different groups against one another, the rise of unverified accounts aggressively promoting divisive narratives affecting an organization and the use of emotionally charged or inflammatory language aimed at inciting conflict.
- **Strengthen Partnerships with External Experts**: Collaborating with external experts in cybersecurity, disinformation analysis and crisis management can provide organizations with specialized knowledge and resources to address and mitigate threats effectively. These partnerships can also help in staying ahead of emerging trends and tactics in the disinformation landscape.

By taking these steps, organizations can better protect themselves from the evolving threat of disinformation, safeguarding their reputation, operations and long-term success. Teneo's Risk Advisory team welcomes the opportunity to speak with organizations to discuss how our deep subject matter expertise, threat-focused approach rooted in structured analytical techniques and robust risk and crisis management experience can help them navigate potential disinformation-related risks and challenges.

Author

Naureen Kabir
Managing Director

For more information, please contact resilience&intelligence@teneo.com.

Teneo Insights | Election 2024 *This article is part of Teneo's ongoing series of conversations around the business implications of the 2024 U.S. presidential election.*

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com