



FLEISHMANHILLARD

CRISIS & ISSUES

Disinformation and misinformation: a communications threat



Disinformation in numbers

2 in 3

Business leaders have experienced false, damaging information about their business being spread online and gaining traction.

FleishmanHillard UK, 2025

\$10.5 tn

The total expected cost of cybercrime in 2025, which is almost 10% of the entire world's GDP (\$115 trillion). The damage from deepfakes alone could reach \$40 billion by 2027.

Deloitte, 2024

<\$5000

To hire bot / troll farms to run a smear campaign on a competitor.

Recorded Future, 2019

A threat to reputation

Misinformation and disinformation attacks represent an entirely new kind of crisis.

Unlike most crises that require an operational-led response from organisations, misinformation and disinformation attacks are a communications first issue.

This distinction matters.

Disinformation campaigns are designed specifically to erode public trust, destabilise credibility and attack the very values of an organisation. They capitalise on moments of crisis to sow confusion and exploit polarising narratives to deepen divisions. They make use of AI generated content, from bot accounts to deep fakes, to turn lies into facts, and weaponise social media algorithms to achieve scale and reach. And, in a world where fake news travels faster than the truth online, the reputational and commercial damage can happen rapidly.

It cannot be ignored. Misinformation and disinformation is the “number one risk that will have the most severe impact on the world over the next two years” says The World Economic Forum’s 2025 Global Risk Report.

Countering disinformation attacks requires a proactive management approach combining crisis communications, reputation management and digital expertise – we can help you protect and respond, starting today.

When is your organisation at risk?

DIRECT ATTACK

False information explicitly targeting a brand, its products or employees to cause reputational and/or financial harm

SECTOR ATTACK

False information about a sector issue and/or competitor is shared online to cause reputational, regulatory, and/or financial harm.

COLLATERAL DAMAGE (INDIRECT ATTACK)

False information about a brand, its products or employees shared online to weaken a political adversary and/or sow societal division and distrust in liberal values. In other words, the politicisation of business.

What makes disinformation stick?

The simplicity and emotional charge of disinformation makes it uniquely potent in capturing attention and fostering engagement. Combined with “plausibility”, the disinformation becomes harder to “shake off”.

Emotional appeal

Evokes strong emotions, often negative, intensifying engagement.

Cognitive simplicity

Lowers barriers to understanding and sharing.

Plausibility

Taps into existing narratives or moments to create a semblance of truth.

How we can help

Coordinated disinformation campaigns are created to cause damage. They put businesses and executives under intense pressure to get it right. Any misstep can significantly escalate the situation. We work with organisations to mitigate and manage disinformation attacks, powered by our data tools.

Prepare

Crisis preparedness including:

- Risk mapping
- Disinformation playbook
- Employee trainings

Digital infrastructure audit including:

Digital audit of your business to:

- Identify potential vulnerabilities to online brand attacks with recommended mitigation measures
- Gaps in infrastructure to strengthen response targeting amid a disinformation campaign

Prevent

Pre-bunking campaigns including:

- Narrative analysis to identify likely mis/dis scenarios.
- Pre-bunking campaign planning including third-party advocates identification, message and content development.
- Campaign launch and live support.

Trust building campaigns including:

- Creation of centralised hub of simple, accurate, accessible information about your business: your single source of truth.
- Trust building campaigns targeting key stakeholders to inoculate them on potential mis/dis.

Respond

24/7 live support, advisory and counsel including:

- Corporate reputation senior counsel
- Real time media/social monitoring
- Stakeholder mapping and live engagement
- Message, content and FAQ development
- Debunking asset development – including videos and graphics
- Platform engagement including paid media strategy
- Full-service, scalable press office
- Crisis media training

Rebuild

Reputation audit & recovery plan including:

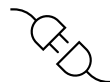
- Polling / qualitative research to assess reputational damage
- Reputation rebuild strategies
- Stakeholder relations campaigns

Lessons learnt workshops

Our team has advised...



... a US automaker on how to protect its reputation from disinformation fuelled during the 2024 US election with a new playbook and protocols.



... a global tech company on its vulnerability to attacks online. We identified that 2/3rds of their social channels were redundant – offering no value yet opening them up to risk.



... a global NGO understand the growing threat of disinformation surrounding vaccines and the development sector and identify mitigatory tactics.



... a pharmaceutical company on developing an issues management framework to identify and combat misinformation amongst patients.



... a global financial institution formalise a process for assessing the threat of disinformation to its business and appropriate response strategies.



... a UK property developer facing an online disinformation campaign from a disgruntled resident targeting the business and its senior leadership team.



... a technology services and consulting company looking to upskill their communications and marketing team on disinformation.



... a UK sports body announce its updated transgender and non-binary participation in competitive sport facing widespread misinformation online.

When to get in touch?

If you answer “no” to one or more of these questions, get in touch today at crisis@fleishman.com.

We want to prepare

Are you clear on what disinformation scenarios pose the greatest risk to your business?

Do you know where your brand appears online?

Do you have a plan in place to mitigate against disinformation campaigns?

Do you know how you would communicate in a disinformation crisis, what protocols and procedures you would use, and who in your organisation is responsible?

Have you trained your communications and marketing team on how to respond to online disinformation and misinformation?

Have you put your crisis management team through the pressure of a real-time disinformation crisis simulation?

We need to prevent

Do you have a plan in place for any potential announcement/issue in the pipeline where there is a heightened risk of disinformation?
High risk scenarios:

- Announcements (products / policies / executive hires / campaigns / partnerships) which intersect with politically or culturally sensitive topics such as ESG and DE&I
- When commenting of geopolitical issues
- Sponsoring global cultural or sporting moments
 - Financial announcements
 - Preparing for litigation – where disinformation campaigns can be used to win the court of public opinion

We're under attack

Do you have a strategy and plan for managing the situation? Are you clear on who is spreading the disinformation and whether bots are involved?

Are you clear on who you need to prioritise communicating with and how best to reach them? Similarly, are you taking proactive steps to disarm critics where appropriate?

Are you clear on what spokesperson to use? Have you identified third-party advocates to amplify your messaging?

Is your messaging landing with your key stakeholders? Is it consistent across channels and addressing everything it needs to be?

Is media coverage balanced and factual?

Do you have the support of your c-suite or Board?

We have to recover

Do you know what the key lessons learnt from the crisis/issue are?

Are you clear on how the crisis has damaged your reputation, and with what stakeholders in particular?

Do you have a recovery plan in place to build back your reputation following the crisis/issue?



FLEISHMANHILLARD

CRISIS & ISSUES

Please get in
touch if you have
any questions.

Thank you.

