COUNTERING CORPORATE DISINFORMATION IN AN AGE OF ESG SCEPTICISM

Authored by: Carys Whomsley (Director) - Digitalis

The notion that companies should be concerned with how their business impacts society and the environment is not new. But in recent years, the impact of businesses on these areas has been at the forefront of public consciousness, influencing consumer behaviour and stakeholder expectations to an unprecedented degree. Activism in this area is gathering pace, with growing concern surrounding the protection of the environment, ethical working practices and human rights.

Demonstrating dedication to environmental, social and governance (ESG) practices is now a key strategy for many corporates. But in the rush to adapt, several have fallen short, with sustainability claims later unmasked as empty rhetoric. This has led to heavy scepticism of ESG claims, which are now closely scrutinised. Greenwashing, corporate hypocrisy and reputation washing – all terms describing the practices of exaggerating ESG credentials – are accusations frequently levelled against companies by the public, and beyond the potential regulatory issues such accusations can bring, they can have devastating and lasting consequences on an organisation's reputation.

Corporates striving to undo decades of unsustainable practices and implement lasting change are acutely aware that it cannot happen overnight.

However, the increasing appetite for change is providing fertile ground for reputational attacks on firms in the form of sensationalist media and social media campaigns. Such approaches can be highly effective in swaying the opinions of consumers who are already angered by the incessant stream of corporate hypocrisy stories.

Stopping the tap on increasingly sophisticated campaigns

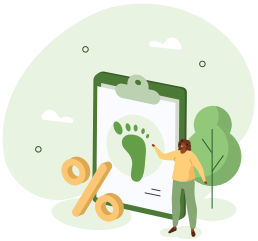
Public sentiment against organisations across multiple sectors is increasingly being manipulated by hostile groups. Coordinated hostile campaigns centred on greenwashing claims are conducted by activists and competitors under the guise of grassroots campaigns or the organic development of consumer concern. The vehicles used for these campaigns are designed to give them broad reach, mixing diverse media to maximise discussion and shareability. Such techniques appear to have been deployed in a fake press release

campaign against Adidas in January this year, which claimed that Cambodian former garment worker and trade union leader was to become its Co-CEO. The group responsible for the fabrication described Adidas as “masters of greenwashing” in explanation of its motive, and the story quickly took hold across traditional and social media outlets.

While the Adidas hoax was rapidly identified as false, the sophistication of disinformation attacks is developing at a frightening pace on social media, and many are not such obvious hoaxes. The orchestrators of these campaigns deploy manipulated media such as deepfakes and false online personas, exploiting new technologies and the limitations of social media platforms’ content moderation capabilities to create and spread the stories. Automated attacks will only become more convincing through the use of new AI software such as ChatGPT, which has already been shown to present misinformation in a deceptively authoritative manner.

With such campaigns proliferating on social media and being promoted through major internet platforms such as Google, all eyes have been on two US Supreme Court cases in February: Twitter v. Taamneh and Gonzalez v. Google. These have led to the examination of the suitability of Section 230 of the US Communications Decency Act, which protects internet providers from liability for the content they carry.

A subsequent bill introduced by a bipartisan group of US Senators and Members of Congress on 28 February 2023, which would make wide-reaching reforms to Section 230, called Safeguarding Against Fraud, Exploitation, Threats, Extremism and Consumer Harms (SAFE TECH), could lead social media companies to be held accountable for enabling forms of online harm including harassment. The outcome will have global implications on the responsibility of tech companies for the content they host – which, one day, may include disinformation.



The complexities of countering hostile campaigns

In the meantime, however, despite the extensive reach of corporate disinformation campaigns on social media and the potential harm that can be inflicted on an organisation’s reputation as a result, countering disinformation can be a slow process – particularly in jurisdictions with weak defamation laws, or when working with unsympathetic social media companies.

As hostile activist and social media campaigns are usually carried out anonymously, it can be difficult to identify their originator(s). The fastest way to prevent a campaign from spreading is often by directly approaching the platforms being used, and demonstrating that the campaign contravenes their terms of use – for example, by proving that coordinated inauthentic behaviour or platform manipulation has taken place. This may involve presenting evidence that participating accounts in a campaign form part of a group of automated accounts known as a botnet, created or co-opted specifically to amplify the hostile campaign. Other approaches may involve presenting evidence of unauthorised and misleading synthetic material, such as deepfakes or doctored photographs, or presenting indications of harassment.

Even if the platforms do agree to take the content down, significant damage may already have been caused by this stage.

A reputation management strategy focusing on communications and legal redress can be essential to mitigating further damage, and recovering resultant financial losses.

Investigative support options for judicial remedies

Digital investigative measures to support an organisation’s legal team are often crucial to ensure the best results are achieved.

The first important measure is preserving all evidence of a campaign as soon as it is identified, and prior to the potential removal of defamatory content on the platforms, to ensure that the potential reach and impact of the narrative can be quantified.

Following this, investigations to establish the spread and reach of the narrative across platforms can provide evidence to show that the threshold for serious harm has been met, for jurisdictions in which this is necessary for defamation claims. Digital investigations can also establish the identities of the individuals or groups behind a hostile campaign, even where they have worked to conceal their involvement. Targeting the originators of a campaign at source can significantly reduce the likelihood of future anonymous campaigns emerging, and close monitoring can ensure that the emergence of any new campaign is stopped in its tracks.

The increased public focus on the importance of ESG matters is a welcome step in the right direction – as is legislator focus on digital trust and safety, placing more responsibility on platforms to prevent the spread of harmful and sensationalist content. But during this adjustment period, it is more important than ever to stay aware of reputational attacks and the best ways to mitigate them.