LEADING THE FIGHT AGAINST DISINFORMATION FOR HIRE

Authored by: Carys Whomsley - Digitalis

Disinformation has become one of the most prominent challenges in navigating the online world. Government bodies, academic institutions, think tanks, and even private companies have researched and proposed innumerable approaches to curb its effects. In this context, defamation lawsuits have emerged as one of the most effective contenders in the struggle against the plague of deceptive information infecting public discourse.

In the early months of 2021, voting technology companies Smartmatic and Dominion Voting Systems filed billion-dollar lawsuits against Fox News in response to the broadcaster's airing of conspiracy theories claiming the companies had rigged the results of the 2020 US Presidential Elections. The companies claimed these false stories had significantly injured their reputations.

Until that point, public pressure and advertising boycotts had achieved almost no perceptible result in combatting the flow of misinformation promoted by right-wing media bodies surrounding the elections. The lawsuits and legal threats had, however, in a matter of weeks, resulted in the cancellation of Lou Dobbs Tonight, Fox Business' highest rated show at the time.

Automated Anonymity

Attributing blame for the spread of a defamatory or false narrative is fairly straightforward when it comes from traditional media channels, where presenters are rarely anonymous personas.

Many people are now, however, flocking to social and alternative media channels as their primary source of information. These channels are highly prone to manipulation, and can be exploited to artificially present any story as credible or widely backed. Automation is cheap and anonymity is easy to achieve, while the platforms themselves are difficult to regulate and moderate.

Under these circumstances, the origin, direction, authenticity and veracity of any circulating story are obscured. Social media has resultingly become one of the most effective tools in propagating targeted disinformation. Empowered by the shield of anonymity, sophisticated, orchestrated attacks on a person or group's reputation can reach millions of people. While the most egregious can be taken down, identifying the attackers themselves for remedial action often seems out of reach.

Covert Operations and Dark PR

Adding to the difficulties in achieving justice for defamatory campaigns playing out online is that many covert influence operations are directed beyond the borders of a target's country.

One powerful tool used in sophisticated campaigns is a practice known as 'astroturfing', in which foreign influence operations masquerade as organic discussion taking place domestically. This type of attack has primarily been seen by actors exploiting political events.

Political leaders and parties have, however, not been the only targets of foreign social media attacks. 'Black' or 'Dark' PR, the practice of destroying a competitor or opponent's reputation through smear campaigns, is increasingly being deployed against organisations and figures in the corporate world. The disinformation for hire market is booming, with services by private contractors offering to manipulate online opinion targeting almost 50 countries last year.

The Network Contagion Research Institute reported that disinformation is increasingly being used against brands and corporations, often through conspiratorial narratives, as seen for example in the 5G conspiracy theories in the UK, which inspired widespread attacks on infrastructure. Companies producing Covid-19 vaccines have been targeted, as has furniture retailer Wayfair, with conspiracy theories gaining enormous traction across Twitter, Facebook and TikTok.

Although the originators of these campaigns are difficult to pinpoint, supportive investigations can nonetheless unearth the real-life identity behind the orchestrators of these campaigns, to expose the attackers and ultimately put an end to the campaign's sway.

Investigatory Methods

Perhaps the most famous investigation into the originators of an influence operation is Robert Mueller's report on Russian interference in the 2016 US elections, the findings of which were achieved through a lengthy process involving subpoenas, search warrants and witness interviews.

Yet several organisations continue to successfully unveil attackers through open-source investigation. The Stanford Internet Observatory, for example, focuses on the identification of foreign influence operations. Its research has led to the takedown of thousands of inauthentic accounts spreading targeted disinformation across multiple social media platforms.

Even the most sophisticated and ostensibly authentic disinformation campaigns leave traces of orchestrated, inauthentic activity. While undetectable to the everyday consumer, investigators can employ numerous tools and methods to confirm the origin, authenticity and modus operandi of these actors.

Influence operations on Twitter, for example, usually take the form of hashtag campaigns. These are achieved by making a hashtag gain enough traction to start trending and reach the desired audience, reinforcing the narrative's apparent legitimacy. To succeed, such operations rely on large bot networks, or 'botnets', created specifically for to spread and amplify the campaign.

Manually creating large enough botnets would be a painstaking process, and may ultimately prove futile if platform moderators find and take down the offending accounts. Botnet creation is therefore most often automated and easily evidenced through shared images, username types and creation dates.

These botnets are often used across multiple campaigns, amplifying the same narratives and relying on key campaign drivers – often accounts under real identities with large followings, which can point to the campaign's true originator.

The New Disinformation Laundromat

Unfortunately, as detection methods evolve, so do tactics to evade them. Disinformation for hire is on the rise, changing the evidence gathering landscape for investigators. With social media campaigns orchestrated by a party in one country, outsourced to a second country and designed to influence a third, the structures behind which the originator of a campaign can hide are becoming increasingly opaque.

Influence operations do however rely on many of the same processes as seen in previous approaches, as the key to a successful disinformation campaign is to make it appear organic enough to generate real engagement. For example, campaigns rely on real individuals, whether paid or indoctrinated, with substantial followings, presenting one avenue for investigators to follow. Separately, the cross-platform nature of these campaigns and reliance on existing perceptions and narratives to be exploited provide other routes into discovering the initiators of these.

The rise of online disinformation is a collective problem with no quick fix, the effects of which will likely only be extinguished through long term educational initiatives. Legal actions and threats have however proved an effective deterrent to disinformation on other media platforms. With investigative support able to unearth actionable intelligence on the leaders of anonymous social media campaigns, a combined approach may offer one solution to put a stop to its ramifications in the meantime.