ISD | Powering solutions to extremism, hate and disinformation

Conspiracy Clickbait: This One Weird Trick Will Undermine Democracy

Elise Thomas

About this publication

In the field of disinformation and conspiracy theories, there has been a tendency for policymakers and practitioners to focus on state-linked operations and to overlook the role of commercially motivated networks. However, the rise of a global industry producing conspiracy clickbait for profit is likely to have significant implications.

This report explores three case studies of how networks linked to individuals in Vietnam are using QAnon conspiracy theories and US political disinformation to generate revenue. These case studies illustrate that although the motive may be commercial, the effect of such networks is to deepen political division and amplify conspiracy theories and disinformation. While each individual network may only have a small impact, the cumulative impact of many such networks around the world may be profound. This growing industry is disproportionately targeted at the US, and therefore should be of particular concern for US policymakers and practitioners.

About the author

Elise Thomas is an OSINT Analyst at ISD, with a background in researching state-linked information operations, disinformation, conspiracy theories and the online dynamics of political movements. She also freelances as a journalist, and her work has appeared in Bellingcat, Foreign Policy, The Daily Beast, Wired and others. She is the author of Recommended Reading: Amazon's algorithms, conspiracy theories and extremist literature and The Long Tail of Influence Operations: A Case Study on News Front and the co-author of COVID-19 Disinformation Briefing No.4.

ISD | Powering solutions to extremism, hate and disinformation

Beirut | Berlin | London | Paris | Washington DC

www.isdglobal.org

Conspiracy Clickbait: Discussion Piece

There is a growing global industry in clickbait conspiracy theories and disinformation, particularly targeting US audiences. While in the past much of the conversation around disinformation and online influence has focused on state-linked actors, profit-driven operations can have equal if not greater impact. The motive may be commercial, but the effect is political.

While not necessarily new – think for example of the infamous Macedonian fake news networks in 2016 – the proliferation of these once-niche operations into a global industry should be cause for concern.

This series has looked at three case studies of networks based in Vietnam which are using QAnon, Covid-19 conspiracy theories, disinformation and divisive political content to target US audiences in order to generate profit. The case studies illustrate the diversity of business models employed by commercially motivated actors. These networks appear to be generating substantial revenue for the people behind them, relative to average incomes in Vietnam. At the same time, the comments left by what appear to be genuine US social media users – which express political polarization and amplify conspiracy theories – demonstrate the political impact.

There has been a tendency to take commercial disinformation and influence operations less seriously than those linked to state-backed actors. This has been the case even where researchers have found state-linked operations are likely to have been extremely ineffective at influencing, or in some cases even reaching, their intended targets.[1]

By contrast and almost by definition, commercial operations are often successful at attracting significant audiences. If they're not successful at doing so, they don't make a profit and the operators move on to something else. Any sustained commercial operation is therefore likely to be reaching at least enough people to make it worthwhile for the operators.

While the frequent deletion of social media accounts makes it difficult to establish exactly how long the three networks in this series have been in operation, their persistence through these deletions is revealing in itself. The fact that they are willing to persevere in the face of repeated deletions and removals indicates that they are generating enough profit to make it worth the time, effort and resources.

That at least two of the networks appear to have pivoted from other content lines to promoting QAnon and other divisive or conspiratorial US political content is also revealing: it suggests a recognition that this sort of content is more likely to drive clicks and generate content than, say, nostalgic TV show content or cute animals. If this same calculation is made by a large number of commercial clickbait operators, the influx of commercially-driven QAnon and conspiracy content into social media platforms would be substantial and concerning.

This situation in which the role of state-linked actors is emphasized while the role of commercial actors is often underplayed bears similarities to the evolution of the ransomware industry. For many years, cybersecurity experts warned that ransomware was moving from a niche skillset into an increasingly low-skill and easily accessible global industry. Despite this, the looming risk was largely overlooked by many for years, in part because it was seen as coming from small-scale commercial operators who were thought of as being neither a major threat or a political concern.

With the benefit of hindsight, it seems abundantly clear that there was a failure to foresee the effects of scale. It's true that the impact of one small cybercrime outfit working out of a back room somewhere is likely to be limited, but when it becomes a thousand, or ten thousand small crews, the collective damage starts to add up significantly. The global cost of ransomware in 2021 is expected to exceed $20 billion,[2] while the human cost in issues like delayed medical care are mounting.[3] Although the motives are commercial, the flow-on impacts have been profoundly political, as the Colonial Pipeline ransomware attack illustrated clearly.[4]

While the contexts are obviously different, the experience with ransomware's evolution from niche skill to globalized industry holds useful lessons for policymakers as online disinformation makes the same transition.

For one, scale matters. Taken in isolation, each of the case studies in this series may reach only a few thousand to a few hundred thousand of people, and their impact may be as fleeting as a single video or post. However, when there are a thousand such networks, or ten thousand or more, everywhere from Nigeria to India to, famously, Macedonia,[5] collectively their reach may be many millions.

For another, there is a difference between political and commercially motivated actors which arguably may result in commercial operators on the whole being more impactful.

State-linked actors sometimes persist in doing the same thing over and over even when it's clearly ineffective at generating engagement. The incentives of the state-linked operators may be more aligned towards pleasing a political hierarchy or hitting KPIs set by their superiors (for example if KPIs are based on producing a certain volume of content, rather than generating engagement) than necessarily achieving a result.

Commercial operators, on the other hand, are strongly incentivized to generate engagement because that's how they make their money. If what they're doing isn't working, they will try new approaches until they find something that does work.

The profit motive explains why so much of this industry is focused on the US, despite the operators being located all over the world. A click from a user based in the US is often substantially more lucrative than a click from a user in a developing country. This means that, while all countries should be paying attention to the development of commercialized disinformation, it should be of particular concern for US policymakers.

This opportunistic, entrepreneurial approach also applies to the type of content it uses to attract users. Fundamentally these are clickbait businesses – and that should worry us.

Consider the way the clickbait industry has, through a steady process of testing and optimization, filled the internet with the cutest cats, or the wildest celebrity rumors, or the most relatable memes. The application of this process of optimization to QAnon conspiracy content, divisive and misleading political news or to public health misinformation is extremely concerning.

Commercial operators are seeking one thing: engagement they can monetize. Hate and outrage are major drivers of online engagement. Another concerning fact is that conspiracy theorists are often hyper-engaged users. Where a person might read one article about a celebrity affair and then carry on with their day, a conspiracy theorist may sit for hours burrowing down the rabbit-hole. This makes conspiracy content an extremely rich vein of engagement for commercial operators to tap.

In Case Study 1, the network appears to have made almost exactly this shift, moving from content about TV shows and cute animals to conspiracy theories like QAnon and divisive political content. This presumably reflects a calculation that there is simply more money to be made in the latter than the former.

As with the ransomware industry, it's important to recognize that non-political motives can still lead to political impacts. These profit-driven networks are amplifying and promoting dangerous conspiracy theories, including smuggling QAnon content onto Facebook despite QAnon ostensibly having been banned from the platform. The comments on this commercially-driven content from US audiences are every bit as polarized, at times violent, and conspiracy-laden as those on 'authentic' QAnon content.

This underscores that when it comes to impact, it doesn't really matter what the network's motive is. As in the example of Case Study 3, operators in Vietnam may simply be making a few bucks off selling a coin, but for the American who buys it, purchasing a 'Trump Revenge Coin' is a political act emblematic of their belief in the Big Lie that the US 2020 election was stolen.

The good news is that at least some of the tools needed to address this already exist. Anti-spam measures implemented by social media platforms appear to be successful in removing at least some components of these networks. However, it is clear that account deletions and takedowns for spam-like behavior will not be enough to deter them from coming back.

Closer cooperation within the social media companies between teams working on addressing spam and influence operations, and perhaps also teams working on other security concerns (for example the abuse of hacked accounts, as seen in Case Study 1) could help to respond to commercial networks with political impacts in a more effective and lasting way.

Commercial actors did not start this fire, but they will fuel it and help it grow. Unless steps are taken to address the growth of the conspiracy clickbait industry, collectively these many small operations are likely to crank up the heat in an already over-heated information environment, creating public discourse which is more politically divisive, more toxic and more riddled with conspiracy theories.

Endnotes

1. Lim, Gabrielle. 'The Risks of Exaggerating Foreign Influence Operations and Disinformation', Centre for International Governance Innovation, 7 August 2020, https://www.cigionline.org/articles/risks-exaggerating-foreign-influence-operations-and-disinformation/
2. Osborne, Charlie. 'The cost of ransomware attacks worldwide will go beyond $265 billion in the next decade', ZD Net, 7 June 2021, https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/
3. Wetsman, Nicole. 'Hospitals say cyberattacks increase death rates and delay patient care', The Verge, 27 September 2021, https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients
4. Sanger, David E and Nicole Perlroth. 'Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity', New York Times, 14 May 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
5. 'The fake news machine: Inside a town gearing up for 2020', CNN, https://money.cnn.com/interactive/media/the-macedonia-story/

ISD | Powering solutions to extremism, hate and disinformation

Beirut | Berlin | London | Paris | Washington DC

www.isdglobal.org