GDI

Global
Disinformation
Index

Adversarial Narratives: A New Model for Disinformation

www.disinformationindex.org

Author: Ben Decker

Editor: Craig Fagan

Design: Dan Smith, www.skyboydesign.com

Acknowledgements: The author would like to thank the following individuals for their review of and guidance on the paper: Yasmin Green (Jigsaw) and Mick West.

The Global Disinformation Index is a UK-based not-for-profit that operates on the three principles of neutrality, independence and transparency. Our vision is a world in which we can trust what we see in the media. Our mission is to restore trust in the media by providing real-time automated risk ratings of the world's media sites through a Global Disinformation Index (GDI). For more information, visit www.disinformationindex.org

GDI Global Disinformation Index

Table of contents

Executive summary

- Today's online threat landscape is significantly more complex and blended, which may lead to many abusive and harmful behaviours slipping through the gaps of current moderation models.
- Disinformation agents, both domestic and foreign, have a large library of content to draw from in crafting new adversarial narratives. In practice this means less overtly fabricated pieces of content.
- Adversarial narratives like "Stop 5G" are effective because they inflame social tensions by exploiting and amplifying perceived grievances of individuals, groups and institutions. The end game is to foster long-term conflict – social, political and economic.
- One key element of these disinformation campaigns is that they contain seeds of factual information that are planted throughout the process.
- As seen in the "Stop 5G" campaign, it is only later on, once you travel away from the original source, that the fabricated conspiracy elements start to be added on.
- Understanding and defending against adversarial narratives requires analysis of both the message's contents and context, and how they are spread through networks and across platforms.

Introduction

The landscape of today's disinformation conflicts online was envisaged over 40 years ago by visionary authors and thinkers.

In Marshall Mcluhan's *Culture is Our Business,* the media scholar predicted that 'World War III is a guerrilla information war with no division between military and civilian participation.'[1]

The seminal piece *Theory of Information Warfare: Preparing for 2020*, written in 1995 by retired Air Force Colonel Richard Szapranski, warned us that the more dependent an adversary is on information systems for decision making, the more vulnerable he is to the hostile manipulation of those systems. Szapranski had the foresight to predict that successful information warfare campaigns would rely on attacking both the knowledge and belief systems of their human targets.[2]

His ideas laid the foundations for the paradigm we know today as fifth generation warfare (5GW). In 2009, a Wired article by David Axe on fifth-generation wars offered additional insights which are chillingly accurate in retrospect: '[T]he next generation of war – the so-called "fifth-generation" – won't feature armies or clear ideas. It will be ... a "vortex of violence," a free-for-all of surprise destruction motivated more by frustration than by any coherent plans for the future. 5GW is what happens when the world's disaffected direct their desperation at the most obvious symbol of everything they lack.'[3]

Since then, we have seen bad faith actors of varying degrees of organisation realising these concepts with troubling success. At their worst, hybrid threat actors embody 5GW principles by combining the promulgation of adversarial narratives online with real world violence. They leverage and exploit network dynamics of platforms to continuously broadcast their message and recruit and radicalise new members through the 'digital influence machine'.[4]

This paper is an attempt to set out a theoretical model for understanding how this 'influence machine' operates and how disinformation is spread. We outline a novel approach for understanding the current state of digital warfare we are in – how adversarial and collective narratives are used for networked conflict. The last part of the paper provides a timely case study involving the adversarial narrative against fifth generation telecommunications networks and the genesis of this disinformation campaign.[5]

Setting out the model: Adversarial narratives

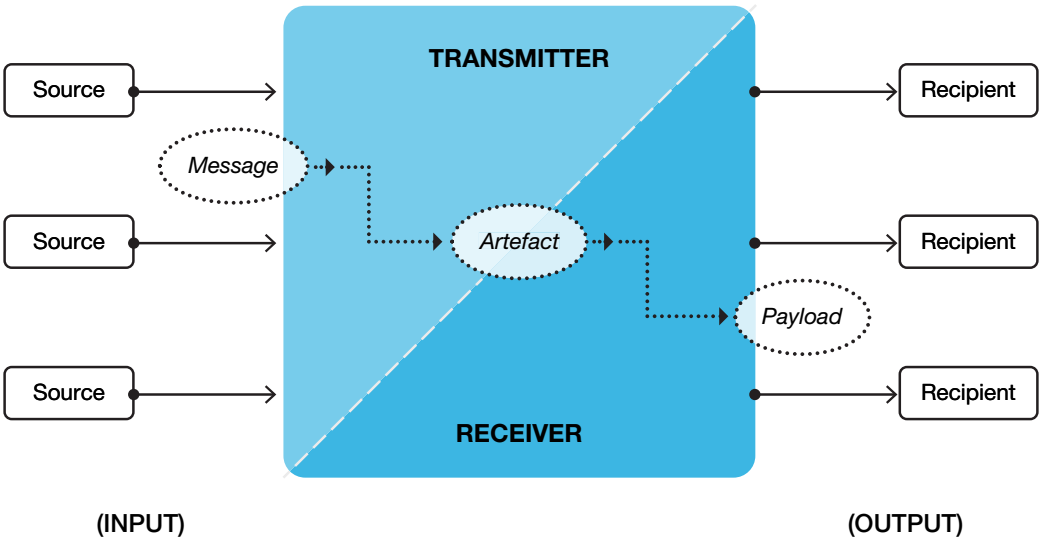
For this paper, we take an expanded definition of platforms to mean all modern online communications domains or platforms that typically function by connecting users to one another in a two-way relationship.

In this sense, platforms are not just the usual suspects like Google, Facebook and Twitter, but include PayPal, eBay, Etsy, LinkedIn and others.

Such a definitional approach is the best way to understand how disinformation is transmitted and received across platforms. For example, many followers of the QAnon conspiracy theory regularly consume content across anonymised message boards like 4chan, 8chan, Voat, and Reddit, post content to more open platforms like Facebook, Twitter, YouTube and Instagram, and, in some cases, sell their own QAnon-related merchandise across ecommerce platforms like Ebay, Etsy and Amazon.[6]

Transmissions generally consist of user-generated content, or 'artefacts', hosted by the system. Moving from left to right in Figure 1, an actor ('source') posts a message on a platform, which is published as content ('artefact') and has the result ('payload') of influencing the behaviour of someone ('recipient').

Figure 1. The Communication Model: The basis for adversarial narratives



Source: Model developed by GDI

The various web artefacts (memes, videos, articles, polls) that are shared between individuals ('source' and 'recipient') fit into a communications framework (i.e. 'distributed narratives'), which can be defined and understood as '"stories that can't be experienced in a single session or in a single space'.[7]

While narratives can be defined as a series of chronological events with some causal relationship, distributed narratives are collections of connected events whose stories are distributed across several platforms in bits and pieces.[8]

Intentionally distributed narratives without a required chronology or sequence of web artefacts, and which seek to enrage and divide internet users, can be defined as adversarial narratives.

Adversarial narratives are rooted in, involve, or are strongly characterised by conflict or opposition between actors and their interests, and especially between a social in-group and an out-group. When adversarial narratives are deployed, they create a series of smaller conflicts played out across the internet.

Adversarial narratives are effective because they inflame social tensions by exploiting and amplifying perceived grievances of individuals, groups and institutions. In the development of the anti-5G narrative, there are kernels of factual legitimacy located throughout its lifecycle. It is only later on, once the narrative begins to travel downstream, that the fabricated conspiracy elements come into play. In many ways, the nature of adversarial narratives makes fact-checking efforts and true/false determinations less effective tools for any counter-messaging strategy. Fact-checks may not counteract the damage done by the original claims nor reach the intended audiences.

Adversarial narratives can be deconstructed into several components that fit within the platform model that we presented above:

- Claims and subclaims: the specific statements which allege 'facts' supportive of the narrative;
- Web artefacts: content that exhibits and transmits related claims and nuanced subclaims (these may be new or recycled); and
- Narrative payload: the overarching narrative that is driven home to the reader of any given artefact. These can be represented as memes, online polls, merchandise, ads and videos (see Figure 2).

Figure 2. Different Elements of the Narrative Payload

Source: Model developed by GDI

With an understanding of the architecture of the narrative payload, we can begin to examine and unpackage the tactics of persuasive manipulation that embody every meme included in the payload. By this we mean Limor Shifman's definition of a meme as 'cultural information that passes along from person to person, yet gradually scales into a shared social phenomenon'.

Therefore, the format of a meme is not limited to manipulated imagery with text overlay. Rather, it is expanded to include all web artefacts ranging from image to video, text, ads and polls, all the way to products sold online. In this context, adversarial memetic influence – the ability to induce a change in the behaviour of another though the use of agitprop or otherwise divisive content – exponentially increases the potential impact of the payload.[9]

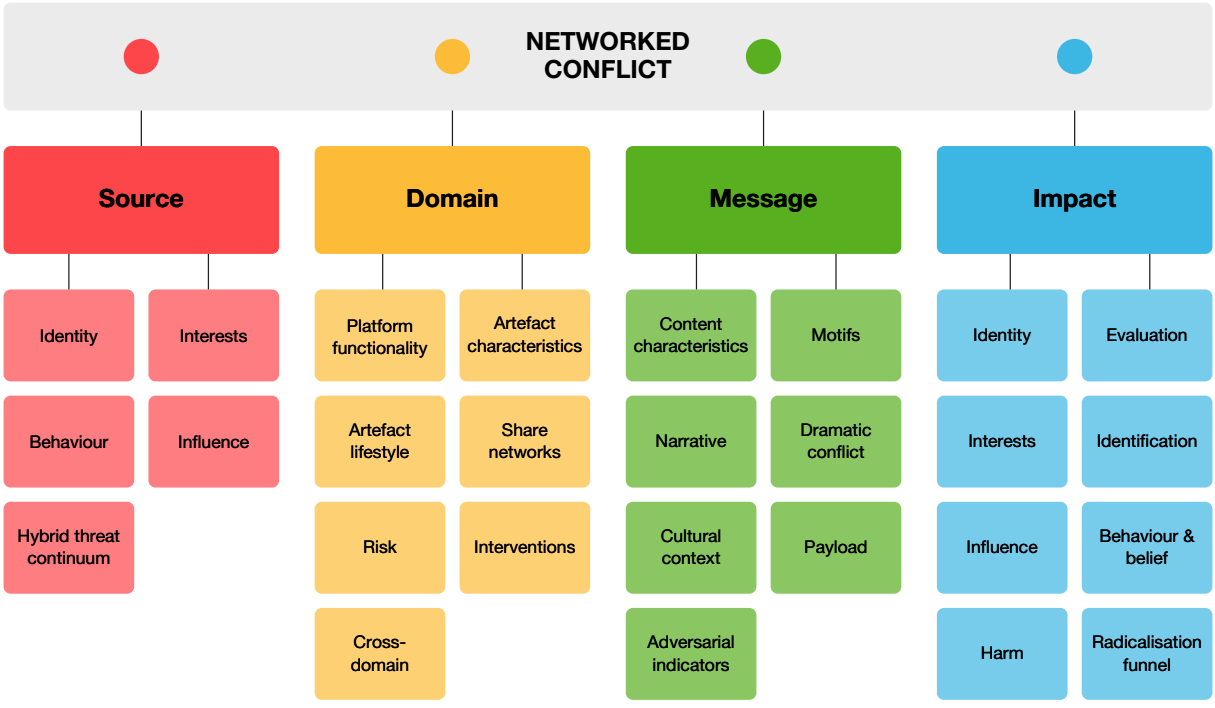
The model: Adversarial networked conflict

Adversarial narratives – which are mob-like and collective – create a networked conflict.

In this context, the conflict takes place over electronic communication networks and employs the tools and functionalities of those systems to influence behaviour. The winners and losers can be defined by the harms and setbacks experienced by one or many parties.

In a networked conflict, a source uses communication domains to transmit a message(s) intended to impact the behaviour of recipients and third parties. Networked conflicts can be usefully analysed by splitting them into four major aspects and multiple component sub-elements: source, domain, message, and impact (see Figure 3).

Figure 3. Networked Conflict and its Components



Source: Model developed by GDI

- **The source** includes the identity, characteristics, interests, and behaviours of the source (whether known or inferred), and its elements may be mapped against hybrid threat model criteria. For example, a source can be a government, private individual(s), or a coordinated group.
- **The domain** includes the functional aspects of the communications platform, as well as the characteristics of artefacts published on and distributed through that system. It also addresses risks posed to the domain, and mitigating interventions which may be applied at the domain level. Here a domain can be an actual site as well as different platforms.
- **The message** includes the contents, motifs, narrative, and cultural context of the message(s) itself, and the payload of the message which influences recipient behaviour. It addresses adversarial uses of narrative and related indicators to drive polarising and divisive behaviours. The term 'message' takes on a new meaning since it looks at the range of different elements used – from posts to Tweets, from memes to videos.
- **The impact** includes the effects on the recipient and third parties of exposure to the message contents, which may include changes in behaviour (influence) as well as actual harms or potential risks of harm to persons. Here, this important distinction lays the groundwork for looking at policy responses – by governments and platforms – to mitigate and prevent such harms.

As we will show later in a case study discussion of the anti-5G movement, conspiracy theorists built up thousands of web artefacts linking mainstream conversations about 5G mobile networks to fringe concepts like the Flat Earth Movement and mind control experiments, by deploying a barrage of Google bombs. These are scores of web links that are used to elevate specific pages to the top of search rankings, exploiting the algorithms and deceiving the general user about the relevance of the search term.[10]

Disinformation agents, both domestic and foreign, have a large library of content from which to craft new adversarial narratives. In practice this means less overtly fabricated pieces of content. Rather, it is a slow and steady diet of manipulated half-truths and veritable information that crescendos into a larger disinformation campaign when a news cycle opportunity appears on an issue that has already been seeded.[11]

This is largely our area of focus: the exploitation and manipulation of algorithms to falsely create a sense that a narrative is more popular than it actually is.

An Adversarial Narrative: The Sepoy Rebellion

The Sepoy Rebellion provides one of the first pre-internet examples of a distributed narrative.

In 1857, Indian colonies grew increasingly concerned about the military, economic, and political control imposed by the British Empire and caught wind of a rumour that the British would impose Christianity on the subcontinent. The first layered narrative came in the form of bread, specifically chapati. In February 1857, a network of clandestine overnight delivery men began distributing chapati breads across India.[12]

Their networked existence began to spark rumours across the country. Some thought that the chapati represented a Christian wafer, and was a warning to the people of India about the British Empire's plans. Others presumed the chapatis had been coated in pork or cow fat and distributed by the British Empire as a means of forced conversion.[13]

The chapatis took on new meaning after the British Army began using a new type of ammunition cartridge for Enfield rifles that required tallow grease, made of beef and pork fat – but which were never given to local Hindu and Muslim conscripts, known as Sepoys.[14]

Historians credit Sepoys for adding to the larger adversarial narrative that the British were attacking the belief systems of Hinduism and Islam. The spread of this rumour among Sepoys sparked a widespread rebellion that lasted over a year. The Sepoy Rebellion highlights the ways in which spatially distributed narratives can be waged by, against, or between social groups of varied technomic capabilities.[15]

Online Narratives: Phenomenon and Effects

Interesting cultural examples that are helpful to understand how adversarial narratives play out in practice online include the Baader Meinhof phenomenon and the Nunes/Streisand effect.

The Baader Meinhof phenomenon, otherwise known as the frequency illusion, is when you learn about something and then it suddenly begins to appear everywhere with a heightened degree of frequency. It was first used in a 1990's online discussion thread on the St. Paul Pioneer Press, 'The first time you learn a new word, phrase or idea, you will see that word, phrase or idea again in print within 24 hours.'[16]

The Nunes/Streisand effect similarly demonstrates our human attraction towards certain types of information, particularly when some individuals prefer we not see it. In 2003, Barbara Streisand sued a California photographer for taking photos of her home in Malibu; however, the lawsuit ultimately drew far more attention to the photos. Streisand not only lost the lawsuit, she unintentionally motivated otherwise ignorant users to consume and share the photos.[17]

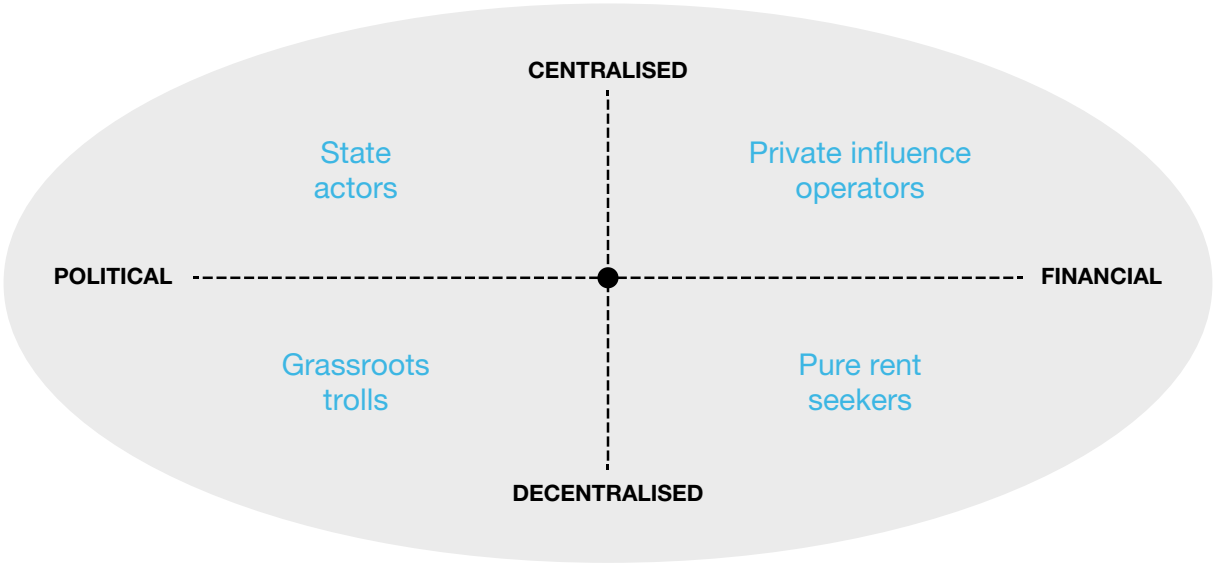
Fast forward to 2019 and it would not be wrong to consider renaming this phenomenon the Nunes effect. In March 2019, California Republican Rep. Devin Nunes sued Twitter, seeking US$ 250 million in damages for what he alleged was defamatory content directed at him online. In the legal complaint, he specifically listed "Devin Nunes' Cow", @DevinCow, as one of the defendants. Before the filing, the Twitter account had less than 1,500 followers. Yet the news of Nunes' lawsuit led to a massive surge in followers, which now totals 621,000.[18]

The disinformation actors

By describing this paradigm as a conflict instead of a war, our definition can include a wider range of hybrid threat agents.

These disinformation actors include state actors, private influence operators, grassroots trolls and pure rent seekers. They can be organised by motivations (from political to financial) and degree of structure (from highly centralised to decentralised), yet they all abuse and exploit adversarial narratives across the web ecosystem.[19]

Figure 4. Disinformation Actors: Range of structure and motivations



Source: GDI and Grace McFadden

Hybrid threat actors intentionally obfuscate the architecture of their digital influence machines. They exhibit a diverse array of characteristics which can be best expressed through a non-binary continuum or gradient of factors. For example, in determining whether or not an adversarial narrative is deploying a Twitter bot network or a Google bomb, inferences about sources may be made based on observable characteristics of public artefacts (e.g., OSINT). The following list aggregates some of these common characteristics.

Hybrid threat actors:
Common characteristics

Ephemeral: Threat actors may move very rapidly, and may leave only ephemeral artefacts of short duration (e.g., platform suspension, or self-deletion).

Gradient of coordination: Coordination can range from little to none, through to active planning and coordination of activities as a group.

Blended authenticity: Hybrid threat agents may combine authentic elements (identities, accounts, beliefs, grievances, real news stories, etc.) with inauthentic elements (fake accounts, satire, false news, etc).

Cross-platform distribution: Attacks may be distributed across multiple accounts and platforms, and where platform enforcement actions occur, they may migrate readily to other platforms to continue.

Peer-to-peer marketing: Threat actors make use of ads, social media posts with no placement cost, and peer-to-peer marketing (influencers).

Global partnerships: Threat actors may themselves be geographically diverse and distributed. They may be state actors in origin (including from overtly hostile as well as allegedly 'friendly' allied nations).

Tacit approval from state actors: Threat actors may receive a range of backing from tacit approval through to material support from states and quasi-state foreign powers.

Financial motivation: Threat actors or private influence networks for hire may run ad networks of distribution, sell merchandise, or receive financial support from their audiences.

Online and offline activities: Activities may consist of a blend of both online and offline actions (e.g., an online campaign supported by allies for and against an issue; violent or threatening offline acts).

Bypass moderation filters: Threat actors may operate just below the threshold of platform rules enforcement – usually intentionally – often through coded language and in-group references (e.g., dog-whistling).

Stop 5G

Our theoretical framework of an adversarial narrative conflict outlines a large marketplace of disinformation being driven by different threat actors.

However, it is often less difficult to talk about a meme or individual threat actor than it is to talk about a distributed network. In the next section, we will apply this model to the adversarial narrative against fifth generation (5G) telecommunications networks.[20]

If we look beyond the news cycle and expand our search to include digital platforms, we can examine 5G through the lens of several digital media buckets:

1. web domains;
2. mainstream social media (Facebook, Twitter, Instagram, YouTube, Reddit, Pinterest);
3. fringe social media (4chan, 8chan, Gab, Voat, Bitchute, etc);
4. ad-tech;
5. ecommerce sites (Etsy, Amazon, TeeSpring, RedBubble);
6. payment platforms (Patreon, GoFundMe, Stripe, Zelle, and PayPal); and
7. cloud and domain service providers.[21]

In examining the chronology of the development of the anti-5G narrative, it is not clear that there is any central unifying provenance. Since 2016, there has been a slow and gradual increase in narrative touch points, including a slew of YouTube uploads, hashtags, Facebook pages, Instagram memes, and web domains, in addition to conversations across fringe and anonymised social networks that include 4chan, 8chan, Gab, and Voat. Without re-creating the entire blueprint for a 5G disinformation narrative, it is important to highlight that conversations began by addressing relevant news topics and social concerns before spiralling out into conspiracy theories.

The initial claims focused on five themes: health, environment, big government, national security, and the economy (see Figure 5). These are all topic areas covered on a daily basis in mainstream and fringe media, which also dominate the talking points amplified by politicians. By design, this framework creates frequent opportunities to weaponise both the news cycle and political rhetoric by inserting more polarising and fabricated talking points before pivoting into full-blown conspiracy theories.[22]

Background

The conversation largely relies on two speeches made by former US Federal Communications Commission (FCC) Chairman Tom Wheeler in June and July of 2016 regarding the rollout of 5G. Much of the criticism of the infrastructure plan hinged upon one theme: how the technology will come to define every vector of our lives.

At the National Press Club in June, Wheeler heralded the adoption of 5G networks and noted that 'Turning innovators loose is far preferable to expecting committees and regulators to define the future.'[23]

Less than one month later, at a press hearing at FCC headquarters on July 14, ahead of the vote to adopt 5G, Wheeler was blitzed by a combination of health risk-related questions.

PHASE 1

Narrative Development (2016–2017)

The first phase, the narrative development, began in the summer of 2016 and spanned the entirety of 2017. Wheeler's quote about regulation became the exploitable piece of verifiable information preyed upon by anti-5G narrative participants.

- ***July 26, 2016:*** Twelve days after the FCC vote, InPower Movement, 'an open source and crowd-funded movement' with 9.3K YouTube subscribers, uploaded 'The Truth About 5G'. The video, which has been viewed over 112,000 times, asks YouTube users, 'Is there a clandestine force working behind the scenes in the United States, censoring truth about the "5G" rollout? Watch this — then decide.'[24]

Figure 5. The 5G Narrative: Mapping of key themes

Source: Model developed by GDI

- ***January 14, 2017:*** Several months later, the Common Sense Show, a fringe influencer on YouTube with 122K subscribers, uploaded 'The New Wireless 5G is Lethal.'[25] The video, which has 44,878 views, featured pre-roll advertising at the time of viewing from Monday.com.
- ***April 14, 2017:*** On Twitter, the first use of #stop5G emerged and included a second fabricated quote from former FCC Chairman Tom Wheeler, '@Susan_Foster: "The deal with 5G? Former FCC Chair Wheeler: 'No time to study health. Billions to be made.' C'mon. It's a 2b #carcinogen. #stop5G #CallReps".[26]
- ***April 22, 2017:*** The first conspiracy claim emerged on #stop5G, '@purestar777, "The Role Of Utility Meters Is to be a Mass Surveillance system" the Internet of Things' #Stop5G https://youtu.be/o7j1Qs01kjA *(video has since been deleted)*.[27]
- ***April – September 2017:*** Over the next several months, search engine optimisation began to improve around anti-5G terms like radiation and cancer links, as fringe influencers increasingly probed open-ended questions relating to the FCC's roll-out of 5G broadband networks under the tutelage of new FCC Chairman Ajit Pai. One of the principal influencers during the incubation phase was conspiracy theorist Max Igan (see box).
- ***October 2017:*** The concept migrates to Reddit's r/conspiracy, a popular subreddit featuring 870,000 members, where it gained increasing toxicity in a post titled "5G and the smart grid is the New World Order".[28]

PHASE 2

Narrative Expansion (2018)

The ultimate objectives guiding success in this phase were twofold: push the narrative payload into the mainstream conversation, and make money off its delivery.

While the #stop5G narrative may have been born in Washington DC, by 2018 it had expanded into a global conversation, leading to the creation of almost 200 Facebook pages and groups, hundreds of YouTube videos, dozens of domains, and a handful of merchandise available for purchase. Fuelling the growth of the narrative payload was no easy task, and involved hundreds of loosely connected or adjacent internet echo chambers. However, there are a few influencers worth highlighting.

- ***January – February 2018:*** John Kuhles, an 'independent "detective like" UFO researcher from the Netherlands, was an early cross-platform adopter of the Stop 5G narrative, creating a digital network that includes multiple web domains, a Facebook Page (13K followers) and Facebook Group (19,617 members), among others.[31] After creating the Facebook page and group in January 2018, he began posting 'stop 5G' videos to YouTube in February and cross-posting to Bitchute, where he could solicit donations from viewers. His websites, stop5G.whynotnews.eu, and stop5G.net, posted daily cannon fodder for his new cross-platform amplification hub.

Who is Max Igan

- His YouTube channel boasts 177K subscribers, which he uses to stoke technology-related fears and concerns about 5G in videos like '5G and the AI Control Grid'.[29]
- Outside of his anti-5G advocacy, Igan is a geopolitical commentator on Press TV, an alleged Iranian state-sponsored propaganda network, and his website, thecrowhouse.com, offers information on a range of conspiracy theories on such topics as China, Israel and 9/11.
- Igan, as his Patreon account would suggest, has a significant financial investment in these conspiracies, in that he is entirely reliant on supporter donations. *'I ask you to please consider that it is only your contribution that keeps me on air, keeps the Crowhouse website going and allows me to continue to produce informative material. I have managed to do the last 8 years mostly with my own funding but now, as much as it pains me to have to do so, the time has come for me to ask for assistance in order to continue.'* [30]

- ***March 2018:*** In the United Kingdom, former footballer-turned-conspiracy theorist David Icke began weighing in, hosting an article on his website '5G: Harmful effects of a new technology',[32] which featured meta tags like mind control and technology. The author of the article, Jon Rappoport,[33] would soon have a chance to traffic the narrative through another influential mouthpiece, Alex Jones.
- ***April 2018:*** Anti-5G websites like stop5G.net and 5Gexposed.com are both registered.
- ***April 4, 2018:*** The article '5G Wireless: A Ridiculous Front for Global Control' was reposted to InfoWars from Rappoport's own website nomorefakenews.com.[34]
- ***May 2018:*** InfoWars created a steady stream of content reinforcing the more threatening secondary narrative, aptly summed up by an Alex Jones Show segment (May 3, 2018): 'YOU HAVE BEEN WARNED: ELECTROMAGNETIC 5G CELL PHONE RADIATION IS DESIGNED TO DECIMATE THE POPULATION'.[35]
- ***May 2018:*** Other conspiracy communities like QAnon began to echo concerns about the negative impacts of 5G smart grids on personal health and the environment.[36] Meanwhile, petitions like 'Stop the Attempted Genocide of the American People with 5G Radiation Cell Towers', posted to WhiteHouse.gov,[37] or 'Let's Make America SAFE Again! No Small Cells in our Neighborhoods',[38] posted to Change.org, and 'Stop 5G!',[39] posted to Avaaz.org, lent further credence to the notion that anti-5G sentiment was increasing in popularity in mainstream conversations.
- ***May 31, 2018:*** RT America broadcast the first of at least eight news segments preying upon concerns about 5G, 'Cancer risk? 5G Wireless speeds could be dangerous'.[40] For state-sponsored media operations like RT, the 5G narrative shows how countries like Russia can pick up on existing disinformation campaigns in an attempt to sow social discord and increase the perception of popularity of certain concepts or sentiments.[41]

PHASE 3

Narrative Deployment (2018-2019)

Over the next several months, a steady stream of content trickled through established networks of propagation, transitioning the narrative payload into its third and final stage, the outbreak. The outbreak can be largely defined by the metastasisation of the narrative payload into national and global media coverage.

- ***October 2018:*** When hundreds of birds died mysteriously at a park in The Hague, John Kuhles, the Dutch UFO researcher, posted on Facebook his own 'evidence-based' article of its link to 5G, which was quoted and shared in November, eventually reaching an estimated 5.7 million social media users.[42] While the story was debunked eight days later,[43] the fact-checked finding reached only an estimated 1.3 million social media users – roughly five times less than the original story.
- ***February 27, 2019:*** TruNews (170K subscribers), whose YouTube channel pledges to offer Christians a positive alternative to the anti-Christian bigotry of the mainstream media, uploaded 'How is 5G Connected to the Mark of the Beast System?' (46,543 views), peppering in anti-Semitism and biblical apocalypse to the payload.[44]
- ***May 12, 2019:*** The New York Times noted that RT had already run seven health-related 5G broadcasts in 2019, often casting it in apocalyptic terms with headlines that include 'A Dangerous 'Experiment on Humanity', '5G Tech is "Crime under International Law'", '"Totally Insane": Telecom Industry Ignores 5G Dangers', and 'Could 5G Put More Kids at Risk for Cancer?'.[45]
- ***May 21, 2019:*** Fox News Host Tucker Carlson raises the question: 'Most of the debate over 5G is centred on China, whether its state-run companies have too much influence in this strategically important field. But there is another even more basic question that has yet to be answered, are 5G networks medically safe?'.[46]

Once deployed, the global news cycle took the narrative payload to unexpected heights when, under the leadership of the US, countries began banning Chinese telecoms giant Huawei from cooperating on 5G network adoption under the veil of national security threats.

Analysis

As the blast radius of the payload expanded with every additional media mention, a loosely defined social media network supporting the 'Stop 5G' narrative used it as daily algorithmic cannon fodder across Facebook, Twitter and Instagram. Using the term 'Stop 5G', we were able to identify 124 Facebook Pages and 74 Groups.

The collective network of 124 Facebook Pages increased its post count from 211 posts/week to 1,019 posts/week during the week of May 19, 2019.

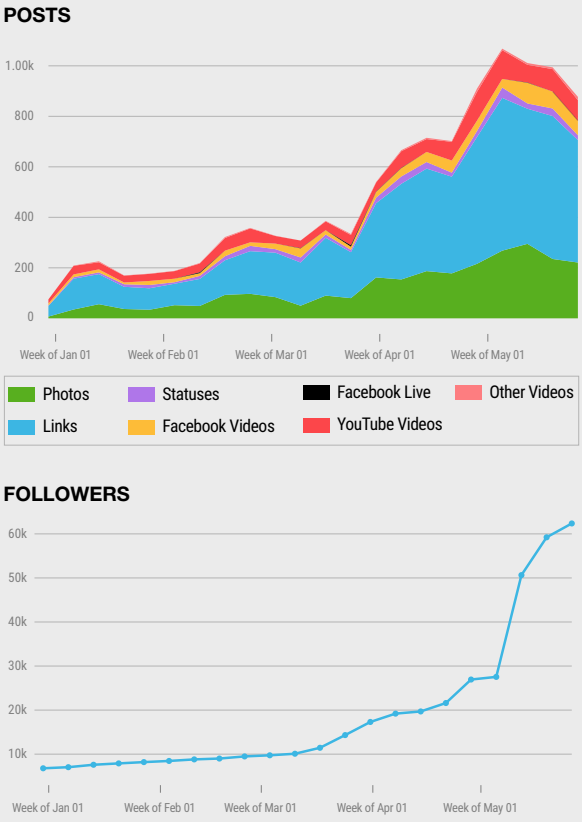
Not only did the post count increase, but the total number of followers swelled from 7,005 to 59,094 during the week of May 12–19 (see Figure 6).

April 2019 was an important inflection point, as the post count began to climb aggressively, while the week of May 12–19 saw an 84 per cent increase in the total number of followers. In examining some of the names of the Facebook pages, the global network effect is clear. Pages were created by groups and users in Australia, Denmark, UK, New Zealand, Scotland, Malta, Italy, Canada, Poland, Ireland, and the United States, among others.

The 74 Facebook Groups experienced similar growth patterns in 2019, with posts per week increasing from 568 posts/week to a total of 3,922 posts/week during the week of May 12–19. Furthermore, the network of Facebook Groups started 2019 with no followers, surging to 50,710 by the week of May 12–19 (see Figure 7).

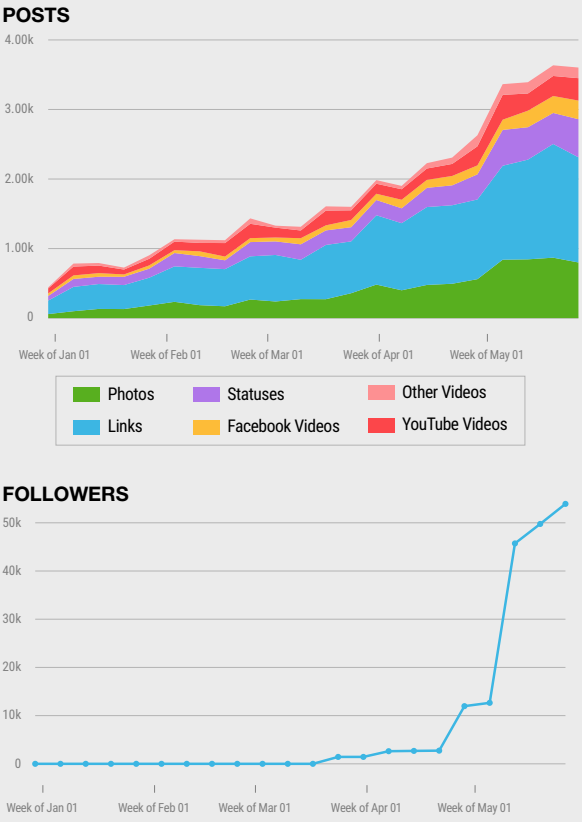
When comparing the arc of the two communities, the page and group audiences both experienced a major increase during the week of May 12–19. While limited access to Facebook data makes any further quantitative analysis an exhaustive manual task, there is a reasonable case to be made that this is more than a coincidence.

Figure 6. Evolution of 'Stop 5G' Facebook Pages – Posts and Followers (Dec – May 2019)



Source: CrowdTangle Intelligence Report 2019

Figure 7. Evolution of 'Stop 5G' Facebook Groups – Posts and Followers (Dec – May 2019)



Source: CrowdTangle Intelligence Report 2019

Outside of Facebook, we began tracking over 600 Twitter accounts using the hashtag #stop5G in 2019 either as a username or in a tweet. The data show markedly similar trends, with an increase in total tweets from 5,058 tweets/week at the beginning of the year, to 16,794 tweets/week during the week of May 12–19, 2019.

Furthermore, the number of followers, which began the year with 314,033, increased to 1.1 million during the week of May 12–19, 2019. Most interestingly, the network increased by 215 per cent during the week of May 12–19, comprising 765,900 Twitter users (see Figure 8).

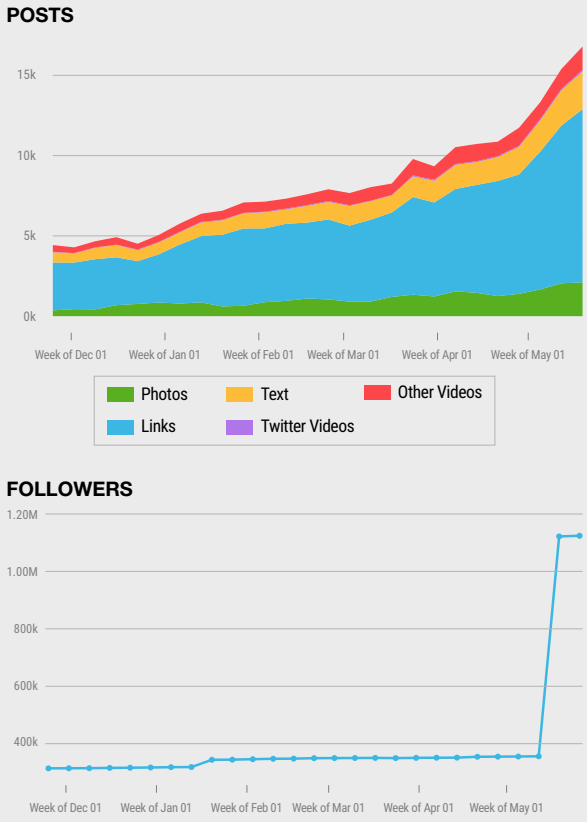
On Instagram, we tracked 43 different accounts featuring 'Stop 5G' in the username, and witnessed similar patterns. The network of accounts, all apparently new, had zero followers at the beginning of May 2019, and almost instantaneously amassed 19,027 followers between May 19–26, 2019 (see Figure 9).

While direct links between the accounts within each network, let alone the links between networks, remain difficult to discern, the suspicious surge in followers across Facebook, Twitter and Instagram came less than a week before Tucker Carlson's Fox News report, when the Google Trend Breakout Score for '5G Radiation' hit 100.

The collective growth point across the aforementioned platforms warrants further investigation, as suspicions of inorganic amplification are more than warranted.

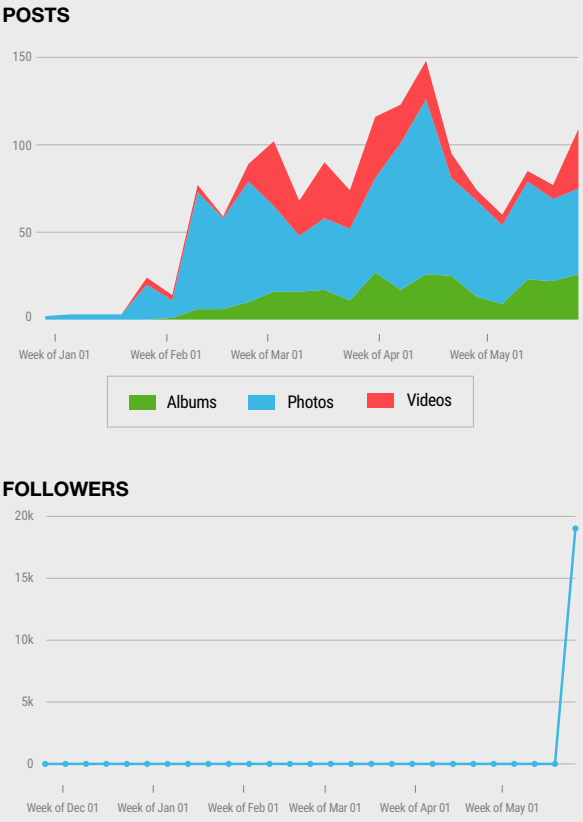
When the amplifiers of this type of content are most effective, they serve as a critical juncture along the path of conspiratorial "red-pilling", i.e. the recruitment of more mainstream and critically-minded individuals to repeat the same narrative.

Figure 8. Evolution of 'Stop 5G' on Twitter – Posts and Followers (Dec – May 2019)



Source: CrowdTangle Intelligence Report 2019

Figure 9. Evolution of 'Stop 5G' on Instagram – Posts and Followers (Dec – May 2019)



Source: CrowdTangle Intelligence Report 2019

Conclusions

Today's online threat landscape is significantly more complex and blended, which may lead to the majority of abusive and harmful behaviours slipping through the gaps of current content and platform moderation models.

Adversarial narratives like 'Stop 5G' are effective because they inflame social tensions by exploiting and amplifying perceived grievances of individuals, groups and institutions. The payload is agnostic to the truth. Rather, the end game is to foster an adversarial narrative conflict, which has become key to the networked disinformation landscape.

In this context, understanding and defending against adversarial narrative campaigns requires analysis of both the message's contents and the context of online information artefacts, and how they are propagated through networks. The need for new approaches to tackle this threat was recently addressed by the New Zealand government's Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online, creating a window of opportunity for change.[47]

Below are some preliminary recommendations for advancing work to diagnose, identify and prevent the new nature of disinformation campaigns:

Diagnose

- Work to define communally agreed-upon online harms arising from disinformation. Such harms include the rise of disinformation and other harmful borderline content leading to radicalisation and violent extremism.[48]
- Agree to rapidly develop initial working definitions, examples, and frameworks for harmful online content for use by platforms and the public.
- Foster the development and implementation of more robust voluntary industry standards around good faith moderation of harmful content online.
- Establish a commission to collaborate on studying and addressing harmful content online.

Identify

- Detect polarising and divisive indicators in content. This approach can be used to detect and escalate potentially risky artefacts matching established criteria.
- Promote robust collaboration on content moderation across social media platforms, cloud service providers and ecommerce providers, among others.
- Share threat intelligence (using harmful content frameworks) with key stakeholders from the platforms, civil society and government (i.e. the ISAC/ISAO model).

Prevent

- Encourage the use of third-party counter-messaging campaigns that directly challenge the adversarial narratives being amplified across the internet on a daily basis.
- Get technology companies and governments to commit to fund, develop, and promote messaging campaigns through the consultation of former members of fringe communities.
- Promote confidential and secure intervention portals for non-profit organisations to proactively reach affected individuals.
- Ensure platforms, brands and ad exchanges work together to demonetise and de-fund disinformation actors and their domains.

The sooner we can come together in establishing shared standards for what constitutes both problematic content and problematic behaviour, the sooner we can approach our social problems head on.

As Sun Tzu once said, 'He who knows the enemy and himself will never in a hundred battles be at risk; he who does not know the enemy but knows himself will sometimes win and sometimes lose; he who knows neither the enemy nor himself will be at risk in every battle.'[49]

Endnotes

1 McLuhan, Marshall. Culture Is Our Business. Wipf & Stock, 2014.

2 Szapranski, Richard. "A Theory of Information Warfare; Preparing for 2020." Airpower Journal, 1995. Accessed June 4, 2019. doi:10.21236/ada328193.

3 Axe, David. "How to Win a Fifth-Generation' War." *Wired*, January 3, 2009.

4 Nadler, Anthony, Matthew Crain, and Joan Donovan. *Weaponizing the Digital Influence Machine.* Report. October 17, 2018. https://datasociety.net/pubs/digital-influence-machine.pdf.

5 Walker, Jill. "Distributed Narrative: Telling Stories Across Networks." *Association of Internet Researchers – Internet Research 5.0*, September 21, 2004, jilltxt.net/txt/AoIR-distributednarrative.pdf.

6 The figures for QAnon products on each are: Ebay: 12,987; Etsy: 825; and Amazon: 603. All figures are as of July 24, 2019. See: Decker, Benjamin T. "Hats and Hate: Merchandising Disinformation Brands." Global Disinformation Index. May 3, 2019. Accessed May 29, 2019. https://disinformationindex.org/2019/05/hats-and-hate-merchandising-disinformation-brands/.

7 Walker, Jill. "Distributed Narrative: Telling Stories Across Networks." *Association of Internet Researchers – Internet Research 5.0*, 21 September 2004, jilltxt.net/txt/AoIR-distributednarrative.pdf.

8 Ibid.

9 Limor Shifman, "Memes in a Digital World: Reconciling with a Conceptual Troublemaker," Journal of Computer-Mediated Communication 18, no. 3 (2013): 362–77.

10 Citron, Danielle Keats. *Hate Crimes in Cyberspace.* Harvard University Press, 2016.

11 Funke, Daniel, and Susan Benkelman. "How Russia's Disinformation Strategy Is Evolving." Poynter. May 23, 2019. Accessed May 29, 2019. https://www.poynter.org/fact-checking/2019/how-russias-disinformation-strategy-is-evolving/.

12 Dash, Mike. "Pass It on: The Secret That Preceded the Indian Rebellion of 1857." Smithsonian Magazine, May 24, 2012. www.smithsonianmag.com/history/pass-it-on-the-secret-that-preceded-the-indian-rebellion-of-1857-105066360/.

13 Ibid.

14 Ibid.

15 Szapranski, Richard. "A Theory of Information Warfare; Preparing for 2020". Airpower Journal, 1995. Accessed June 4, 2019. doi:10.21236/ada328193.

16 In 2006 linguistics scholar Arnold Zwicky expanded upon the definition in his research on the three linguistic illusions relevant to cognitive biases. See: Zwicky, Arnold. "Just between Dr. Language and I." Language Log, University of Pennsylvania, September 10, 2005. itre.cis.upenn.edu/~myl/languagelog/archives/002386.html.

17 Holiday, Ryan. “Conspiracy: Peter Thiel, Hulk Hogan, Gawker, and the Anatomy of Intrigue”. NY, NY: Portfolio/Penguin, 2018.

18 Twitter followers for @devincow are as of July 24, 2019. See: Cuthbertson, Anthony. “Republican Congressman Sues Twitter for $250m after Parody Account of His 'Mom' Insults Him.” The Independent, March 19, 2019, www.independent.co.uk/life-style/gadgets-and-tech/news/devin-nunes-twitter-lawsuit-parody-mom-republican-a8829496.html.

19 Melford, Clare, and Craig Fagan. "Cutting the Funding of Disinformation: The Ad-Tech Solution." Global Disinformation Index. May 2019. Accessed June 3, 2019. https://disinformationindex.org/wp-content/uploads/2019/05/GDI_Report_Screen_AW2.pdf.

20 Walker, Jill. “Distributed Narrative: Telling Stories Across Networks.” *Association of Internet Researchers – Internet Research 5.0*, September 21, 2004. jilltxt.net/txt/AoIR-distributednarrative.pdf.

21 Decker, Benjamin T. "Hats and Hate: Merchandising Disinformation Brands." Global Disinformation Index. May 3, 2019. Accessed May 29, 2019. https://disinformationindex.org/2019/05/hats-and-hate-merchandising-disinformation-brands/.

22 Boyd, Danah. "Media Manipulation, Strategic Amplification, and Responsible Journalism." Speech, Online News Association Conference 2018, Austin, Texas, September 14, 2018. https://points.datasociety.net/media-manipulation-strategic-amplification-and-responsible-journalism-95f4d611f462.

23 Wheeler, Tom. “The Future of Wireless: A Vision for U.S. Leadership in a 5G World.’” National Press Club. Washington, DC, transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0620/DOC-339920A1.pdf.

24 See: https://www.youtube.com/watch?time_continue=309&v=OMxfffqyDtc.

25 See: https://www.youtube.com/watch?v=9fpNPZVVMho.

26 We could not find any direct quote from Wheeler based on the Tweet; however, as a helpful example of narrative recycling, cell phone radiation activists have been making similar claims that the former FCC chairman had been suppressing cell phone radiation research since at least November 2013. See: www.rfsafe.com/tom-wheeler-new-chairman-of-the-fcc-suppressed-research-on-the-health-effects-of-cell-phone-radiation/. Also see: https://twitter.com/Susan_Foster_/status/852953011827597312.

27 See: https://twitter.com/purestar777/status/855983298287247361.

28 See: https://www.reddit.com/r/conspiracy/comments/76g84r/5g_and_the_smart_grid_is_the_new_world_order/.

29 For more information, see: https://www.youtube.com/channel/UCegOTmclzjfKuQh0SHflqww, https://www.youtube.com/watch?v=bY3CVNxWwVs, and https://thecrowhouse.com/home.html.

30 See: https://www.patreon.com/maxigan.

31 See: https://bbsradio.com/untoldmysteries, https://www.facebook.com/Stop5G/ and https://www.facebook.com/groups/stop5g/.

32 See: https://www.davidicke.com/article/465686/5g-harmful-effects-new-technology.

33 Rappoport still maintains an active presence on Twitter (23.1K followers), Gab (1,362 followers), and Minds (182 subscribers).

34 See: https://www.infowars.com/5g-wireless-a-ridiculous-front-for-global-control/.

35 Jones, Alex. "You Have Been Warned: Electromagnetic 5G Cell Phone Radiation is Designed to Decimate the Population." InfoWars. May 3, 2018. Accessed June 7, 2019. https://www.infowars.com/you-have-been-warned-electromagnetic-5g-cell-phone-radiation-is-designed-to-decimate-the-population/.

36 See: https://twitter.com/against5g/status/1000997523807387648?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7.

37 See: https://petitions.whitehouse.gov/petition/stop-attempted-genocide-american-people-5g-radiation-cell-towers.

38 See: https://www.change.org/p/let-s-make-america-safe-again-no-small-cells-in-our-neighborhoods.

39 See: https://secure.avaaz.org/en/community_petitions/Everyone_who_is_concerned_about_the_proven_health_dangers_of_5G_STOP_5G/.

40 See: https://www.youtube.com/watch?v=TmLwuM0_MJg.

41 Funke, Daniel, and Susan Benkelman. "How Russia's Disinformation Strategy Is Evolving." Poynter. May 23, 2019. Accessed May 29, 2019. https://www.poynter.org/fact-checking/2019/how-russias-disinformation-strategy-is-evolving/.

42 Elizabeth, Erin. "Hundreds of Birds Dead during 5G Experiment in The Hague, The Netherlands." Health Nut News. November 6, 2018. Accessed May 29, 2019. This story was reposted to InfoWars and shared on social media pages like Qanon, AntiVaxxers, Yellow Vests International, and Anonymous, as well as a network of "Stop 5G" Facebook pages. https://www.healthnutnews.com/hundreds-of-birds-dead-during-5g-experiment-in-the-hague-the-netherlands/. The article's reach is based on CrowdTangle figures.

43 Kasprak, Alex. "FACT CHECK: Did a 5G Cellular Network Test Cause Hundreds of Birds to Die?" Snopes.com. November 13, 2018. Accessed May 29, 2019. https://www.snopes.com/fact-check/5g-cellular-test-birds/.

44 Burke, Timothy. "Far-Right Show TruNews Warns: 5G Technology Is the Antichrist." The Daily Beast. February 28, 2019. Accessed May 29, 2019. https://www.thedailybeast.com/far-right-show-trunews-warns-5g-technology-is-the-antichrist. Also see: https://www.youtube.com/user/TRUNEWSofficial/about and https://www.youtube.com/watch?v=fqCMb9NAQ2o&t=2s.

45 Broad, William J. "Your 5G Phone Won't Hurt You. But Russia Wants You to Think Otherwise." The New York Times, May 12, 2019, www.nytimes.com/2019/05/12/science/5g-phone-safety-health-russia.html.

46 Carlson, Tucker. "Are 5G Networks a Danger to Our Health and Safety?" Fox News. May 21, 2019. Accessed May 29, 2019. https://video.foxnews.com/v/6039592759001/#sp=show-clips.

47 "Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online." *Christchurch Call*, New Zealand Ministry of Foreign Affairs and Trade, May 15, 2019, www.christchurchcall.com/call.html.

48 Johnson, Eric. "Tristan Harris Says Tech Is "downgrading" Humanity - but We Can Fix It." Vox. May 6, 2019. Accessed May 29, 2019. https://www.vox.com/recode/2019/5/6/18530860/tristan-harris-human-downgrading-time-well-spent-kara-swisher-recode-decode-podcast-interview.

49 Sun-tzu, and John Minford. "The Art of War". New York: Penguin Books, 2002.

GDI Global Disinformation Index

www.disinformationindex.org