



GDI

Global
Disinformation
Index

Cutting the Funding of Disinformation: The Ad-Tech Solution

www.disinformationindex.org



Authors: Clare Melford and Craig Fagan.

Contributors: Sophie Chauvet, Ben Decker, Sam North and Danny Rogers.

Design: Dan Smith, www.skyboydesign.com

Inside cover photo: Joshua K. Jackson on Unsplash.

Acknowledgements: The authors would like to thank the following individuals for their review of and guidance on the paper: Miguel Martinez (Signal AI), Connie Moon Sehat (Credibility Coalition), Alexandra Mousavizadeh (GDI), Lisa-Maria Neudert (Oxford Internet Institute), Peter Pomerantsev (London School of Economics) and Scott Yates (Certified Content Coalition).

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



May 2019. Published under a Creative Commons License (CC BY-NC-SA 4.0)

Table of contents

Preface	4
Introduction	5
Bad intentions: The actors behind disinformation	6
A perfect storm: How did ad-tech get here?	9
A system abused: The money and the messages of disinformation	12
The GDI method	17
The way forward	21
Endnotes	22

Preface

The world wide web turned 30 years old in 2019. Since its invention, how we live our lives online – and off – has changed in countless ways.

The web has brought us closer together, expanded our knowledge, opened up our societies and broken down barriers for billions of people around the world. But being more ‘networked’ and ‘connected’ has come with its own dark sides. Disinformation is one of them.

Disinformation has been used as a tool to weaponise mass influence and disseminate propaganda. It has brought extreme fallout for economies, politics and societies around the globe. No country is immune.

Disinformation has become public enemy number one in many parts of the world. A wave of regulations to deal with the problem is brewing from Australia to the United States. But the issue is a deep one that regulations alone will not solve. To combat disinformation, we need to understand efforts to disinform – both upstream (where disinformation starts) and downstream (where and how it spreads). This is where the Global Disinformation Index (GDI) has set its focus.

For the GDI, financial motivation is a connecting point that links together the upstream and downstream components of disinformation. To substantially reduce disinformation, we need to disrupt its funding and remove the financial incentive to disinform. This means turning our attention to the ad-tech industry. Ad-tech has inadvertently thrown a funding line to disinformation domains through online advertising. Until now, there has been no way for advertisers to know the disinformation risk of the domains carrying their ads. The GDI aims to change this state of affairs. The paper that follows explains why this shift is needed – and how the GDI can trigger it.

The GDI aspires to offer a trusted and neutral assessment about a news domain’s risk of disinforming. By looking at metadata, contextual and content flags, the GDI will provide a domain-level rating about its risk of disinforming a user. We are in the process of building the index and will pilot it in a limited number of countries by early 2020. In the coming months a proposed methodology will be published for review by the community.

We are designing the GDI from the bottom up on the three pillars of neutrality, independence and transparency.

- **Neutrality:** We are apolitical, global, and evidence-based. We are establishing a governance structure which aspires to the highest standards of global corporate governance.
- **Independence:** The GDI is established as a not-for-profit entity. We receive no benefit from the risk ratings we give to a particular site. We exist solely to assess online news domains’ risk of disinforming their readers.
- **Transparency:** The GDI’s rating criteria, assessments and methodology will all be community-driven and made publicly auditable. A dispute mechanism will be developed and made available for the owners of domains that disagree with their rating.

We look forward to having you join us on this journey to combat disinformation.

Introduction

Disinformation is often talked about as a thing, a piece of content, an output. But it is also, and more perniciously, a process.

The verb (to disinform) gives us new perspectives into the noun (disinformation).¹ For the Global Disinformation Index (GDI), it is our focus to understand, assess and rate the risk of domains that disinform. The index uses both automated and manual means to determine such risks. GDI defines ‘to disinform’ as: to purposely and/or maliciously mislead by spreading inaccurate information (in terms of the content itself and the context).

The ad-tech system is currently supplying oxygen – and money – to domains that disinform. This is happening inadvertently through online adverts being placed on domains that disinform, which is providing these domains with funding and a platform to amplify their messages. It is time to follow the money of disinformation.² This approach is different from – and adds to – the growing body of work on disinformation actors.

To combat efforts to disinform, we must understand the process and motivations behind it. The motivations to disinform may be political, financial or a combination of both. At GDI, we focus on removing the financial incentives. We believe that by working with the online advertising system to use GDI ratings in their ad spending decisions, we can quickly cut the financing lifeline to domains that disinform. These domains often include numerous ‘junk’ news sites set up simply to get page views and ad clicks. Cutting off their ad monies will increase friction and create obstacles for disinformation actors – including those with political motives – to spread their messaging online.

The ad-tech system needs a way to classify domains by their risk of disinforming users. This is what the GDI proposes. The index focuses on the domain level to identify disinformation risks, by automatically and manually analysing domains’ metadata and other observable factors. Measuring these different elements over time allows the GDI to be updated continually and fed into the ad-tech system, in order to redirect ad monies in real time away from junk news domains and towards high-quality news sites.

The GDI aims to benefit brands and other actors in the ad-tech ecosystem. The GDI risk ratings aim to provide a neutral, transparent and independent assessment to clean up the ad-tech ecosystem and promote brand safety.

With the GDI ratings:

- **Brands and media agencies** will have a better understanding and greater control over whether their advertisements are being placed on risky sites.
- **The ad-tech community** will have non-biased feedback to direct ad money away from domains with high disinformation risks.
- **Social platforms and search engines** will have neutral ways to encourage the spread of information and rein in disinformation efforts.
- **Online users** will have greater context about the domains which they read, comment on, and share.

Everyone in the ecosystem needs to work together to undo the perverse incentives that have enabled disinformation actors to feed off the ad-tech ecosystem, and to find ways that better provide funding for and rebuild the credibility of high-quality news domains.³

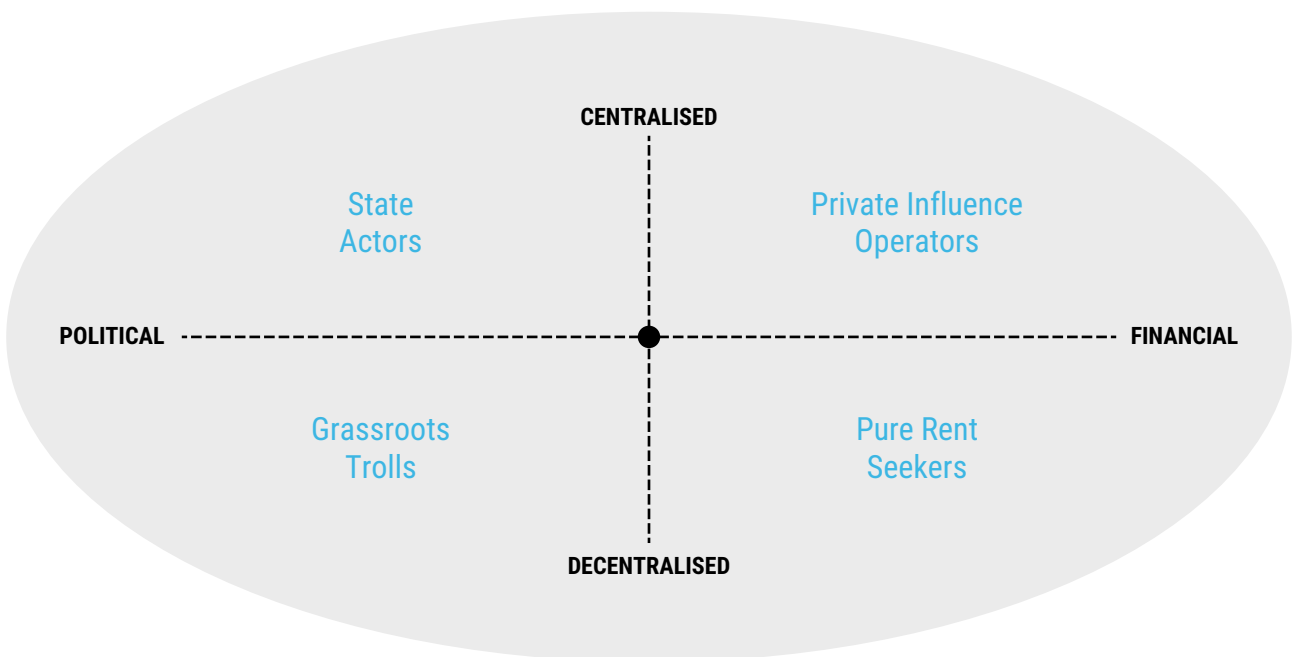
Bad intentions: The actors behind disinformation

Disinformation actors are an old problem. What's new is the breadth, depth, speed and reach of their actions.

Some disinformation actors are able to test and iterate their messaging and content very quickly, often as news and events are unfolding in real time. Rather than a single source for a single message⁴, disinformation in today's world can mean that multiple sources are simultaneously broadcasting the same disinformation throughout multiple networks and via multiple media.

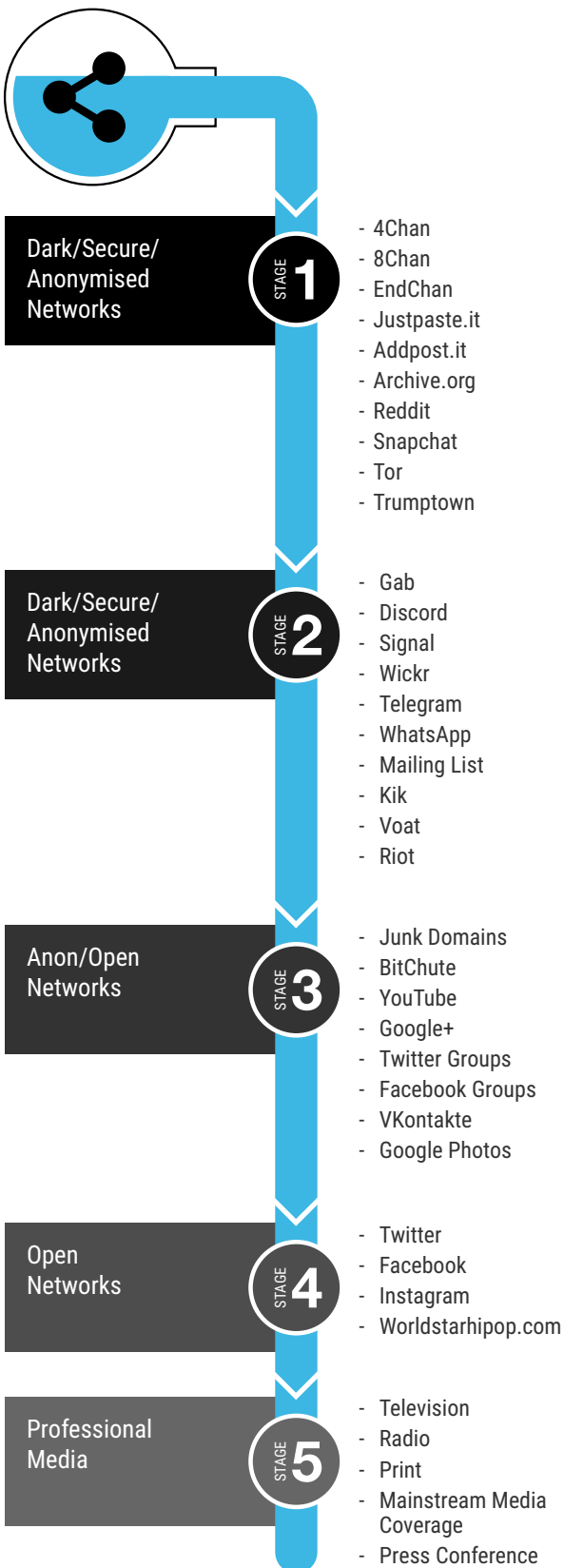
Disinformation domains – and the actors behind them – have different motivations. One actor's intent might be simply to get more site traffic and increase ad revenue. Another's intent might be to sway political opinions and votes. Or another actor might be doing it as part of a targeted campaign (i.e. commercial or political). Others might be doing it just for the 'lulz'.

GDI divides these four different actors into four quadrants, organised by their motivations (from political to financial) and by their degree of structure (from highly centralised to highly decentralised). They may have different end goals (money or engagement), but all of these four actors abuse the ad-tech system in similar ways.



Source: GDI and Grace McFadden

Figure 1: The Troll Flow



Source: Model developed by Benjamin T. Decker/GDI

State actors: These include governments as well as state-linked actors that push government propaganda. These actors use online channels as well as traditional media (radio, tv and print). Centralised actors have always been active in the disinformation space – including reportedly the UK in the 1960s⁵ or the US in the early 2000s.⁶ But centralised actors have gained a new reach and virality for their messages online. Often they have no need to rely on ad-supported funding. Since 2010, a wide range of governments have been accused of questionable online actions, with many aimed at spreading inaccurate information.⁷ More recent examples of efforts to disinform include those by China⁸, the Philippines⁹, Iran¹⁰, Russia¹¹, South Africa¹², and Venezuela.¹³ In March 2019, Facebook removed many news-related pages, groups and accounts seen as linked to ‘inauthentic behaviour’ with operations ‘connected to Iran, Russia, Macedonia and Kosovo’.¹⁴

Private influence operators: These are for-hire companies such as the now-defunct Cambridge Analytica, which run commercial marketing and public relations campaigns that aim to disinform for their high-paying clients. Their schemes may involve a specific psychological, behavioural or political agenda or campaign. Or they may be designed for the highest bidder. They tend to produce professional-looking, ad-supported domains that mimic traditional journalism. Recent examples include allegations of a disinformation campaign against the current president of Mexico¹⁵ and disinformation tactics employed in India’s conflict with Pakistan.¹⁶

Grassroots trolls: These are often individuals or groups that come together around a specific issue or cause such as #gamergate or #pizzagate.¹⁷ Their content and activities may focus on hate speech or abuse, or they might try to push a false narrative to credible journalists and media outlets. They may start out on forums like 4chan or 8chan, move to other intermediate platforms like Reddit and finally into mainstream media (see Figure 1). They may have a specific ideological agenda or they might just do it ‘for the lulz’. Recent actions have been diverse. Trolls have even used online comments to push agendas, such as on movie or book review platforms.¹⁸ They have tried to manipulate online voting systems to skew results, such as in a documented attack against an all-female, African American team vying for a prestigious high school science award in the US.¹⁹

Pure rent-seekers: This group is only after the clicks and the money that goes with them. They want to drive visitors – and also bots – to their sites so that they can collect on adverts. They often use clickbait or sensationalist language and images, and sometimes even ad arbitrage.²⁰ Clickbait factories have been set up by ‘fake news merchants’ in countries like Bangladesh²¹, Macedonia, and Kosovo²² to churn out disinformation, blasting headlines and earning a few thousand dollars or euros each day.²³

At GDI, we believe that we need to understand these four quadrants of the threat spectrum in order to disrupt the systems that allow actors to disinform. At times,

the interests of disinformation actors in these various categories overlap, and they often rely on each other to amplify their messages. This means that even actors that are not directly dependent on ad revenue would likely be weakened by a disrupted flow of ad monies to others in the disinformation cycle. For example, many political conspiracies originate in fringe networks that depend on financially-motivated domains to legitimise their content.²⁴ Interfering with domains that bridge fringe and mainstream networks could make it more difficult for disinformation to grow and spread.

This is why we need to find ways to neutralise the ad-tech structures that disinformation actors are abusing.

CASE STUDY

Seven False Canadian News Sites, One Ukrainian Man and US\$1,300 in Monthly Ad Revenues

According to a CBC investigation by Canadian journalist Jeff Yates in 2017, at least seven false Canadian journalism outlets²⁵ have been identified as part of an advertising revenue-generating scheme based in Ukraine. This puzzle was pieced together thanks to information that he found, which linked all of the sites back to the same Google AdSense account and showed that they all had similar layouts. Masquerading as local Canadian websites, they published poorly translated articles targeted at the province of Quebec. One of these sites, called *The Siver Times*, publishes content in English, German and French.²⁶

What made these sites a source of disinformation is how they maliciously distorted the context of the sites and articles to dupe readers. They all passed themselves off as local provincial papers. Some of the articles on the sites were directly plagiarised. One of the websites, *The Sherbrooke Times*, used the image of a supposedly local church that is actually a cathedral in Brussels.²⁷ Others propagated age-old conspiracy theories, such as alleging that NASA had doctored the Apollo 17 landing on the moon.

Their content has been shared and amplified – by people and bots.²⁸ Some of the most viral articles have been shared most by people living outside of Quebec. For example, Jonathan Cerrada, a Belgian

singer, and Anne Marie Waters, a UKIP anti-Muslim activist in the UK, have shared some of the articles. At the same time, a network of 300 Russian bots has reportedly been found spreading the stories.

Through Yates’ investigation, it was found that all the sites were registered to Ukrainian addresses. The websites also turned out to be hosted on Ukrainian and Russian servers.

The person behind these websites was identified as a 38-year-old Ukrainian man who lived off the sites’ programmatic ad revenues.²⁹ Estimates show that based on site traffic, the combined sites could have generated roughly US\$1,300 a month in income.³⁰ This amount is equivalent to four times the average monthly salary in Ukraine. However, when the original story was reported, Google deactivated their shared AdSense account for violating platform policies.

The fact that these websites specifically mimicked local outlets is troubling. Like in the US, Canadians tend to have greater trust in local news outlets than national media.³¹ Disinformation sites masquerading as local media have also been documented across the border in the US.³²

A perfect storm: How did ad-tech get here?

Four seismic developments have transformed the online advertising world in the past decade.

These four trends have created a perfect storm, allowing malicious actors unprecedented reach, precision and rewards for their messages that disinform:

TREND 1:

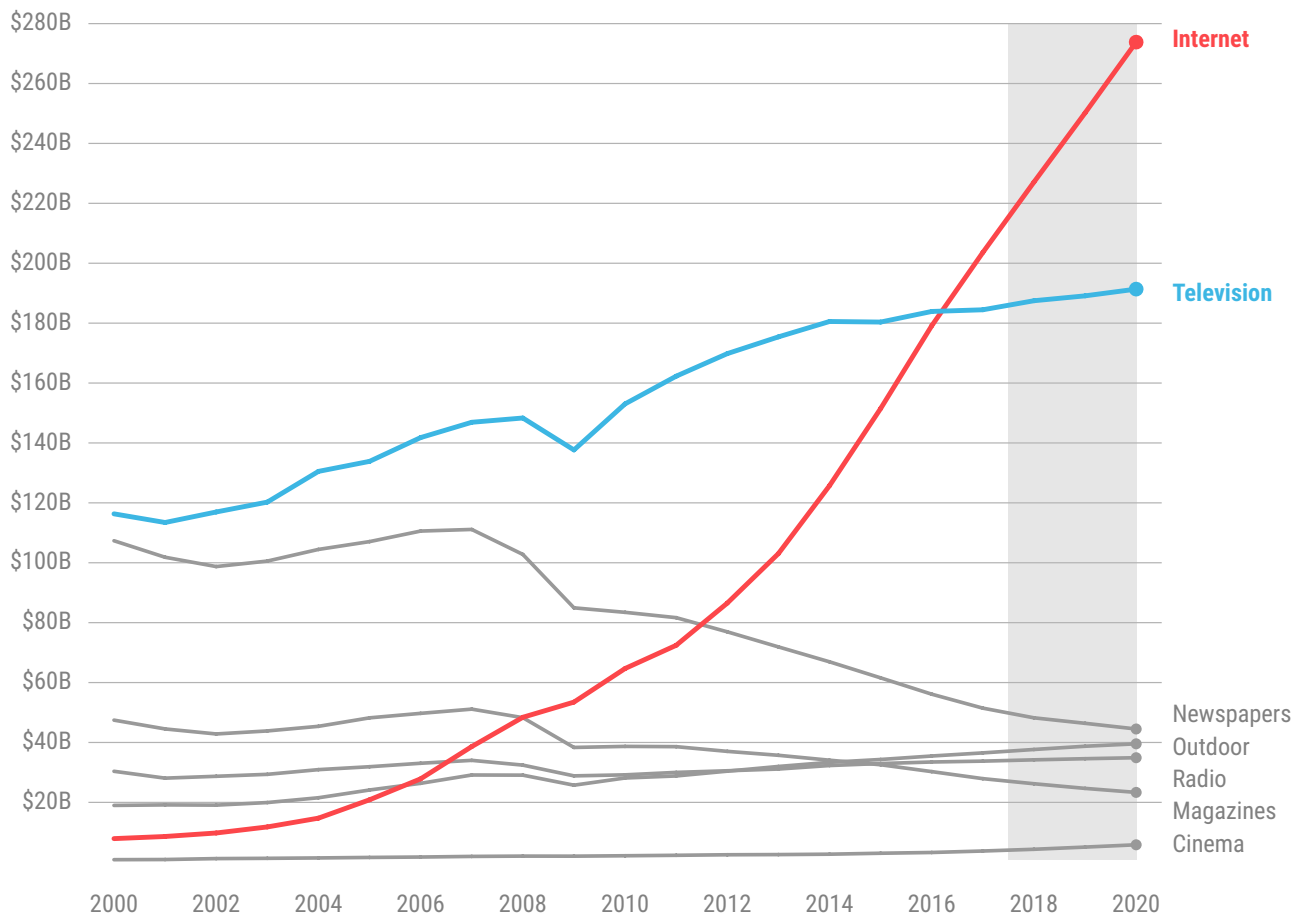
Online media sources explode as media trust sputters. Media content creation has been decentralised, democratised and multiplied. Hundreds of hours of new content are uploaded to YouTube every minute. An average of 6,000 tweets are sent out every second.³³ In the time it has taken you to read this section (about 10 seconds), Facebook users around the world have liked over 660,000 posts.³⁴ With all of this content, many more people now turn to these platforms to get their news – in formats that are usually lacking the typical signifiers of the information’s source and trustworthiness (like a brand name or masthead). More than two-thirds of people in highly connected countries like Argentina³⁵, Malaysia³⁶, Mexico³⁷, and the US³⁸ get their news from social platforms rather than any direct news source. But a greater number of sources for content does not necessarily mean more trusted content – or trust in media. Overall, media is the least trusted institution in the world.³⁹ And only 43 percent of people surveyed trust social media for general news and information.⁴⁰

TREND 2:

Advertising money floods the online space. This deluge of money from brands started in the mid-2000s. The shift has led to declines in advertising (or slower growth) on other media. 2016 was the first year in which online ad spends actually surpassed those on television⁴¹, reflecting the gold rush into ad-tech (see Figure 2). It is predicted that between now and 2020, two-thirds of the expected growth in global advertising will come from online spends on paid search and social media ads.⁴² In countries with nascent online ad markets like Indonesia, Mexico, Russia, and Brazil, digital ad spends will continue to see double-digit growth, bringing opportunities and risks to brand safety in these markets.⁴³

Yet brands are not the only ones that are spending. Political ad spending has increased exponentially over the same period, but without adequate oversight. Mexico’s presidential election in 2018 saw candidates lay out nearly one-third of their ad spend on digital media.⁴⁴ One estimate suggests that across US campaigns in 2018, US\$1.9 billion was spent on digital and online political campaigns. In 2014, this figure was US\$71 million.⁴⁵ In the UK, digital spends by political campaigns in 2018 accounted for nearly 43 percent of their advertising costs, a forty-fold increase in four years.⁴⁶

Figure 2: Evolution of Ad Spend, 2000-2020 (US\$)



Source: <https://www.recode.net/2018/3/26/17163852/online-internet-advertisers-outspend-tv-ads-advertisers-social-video-mobile-40-billion-2018>

TREND 3:

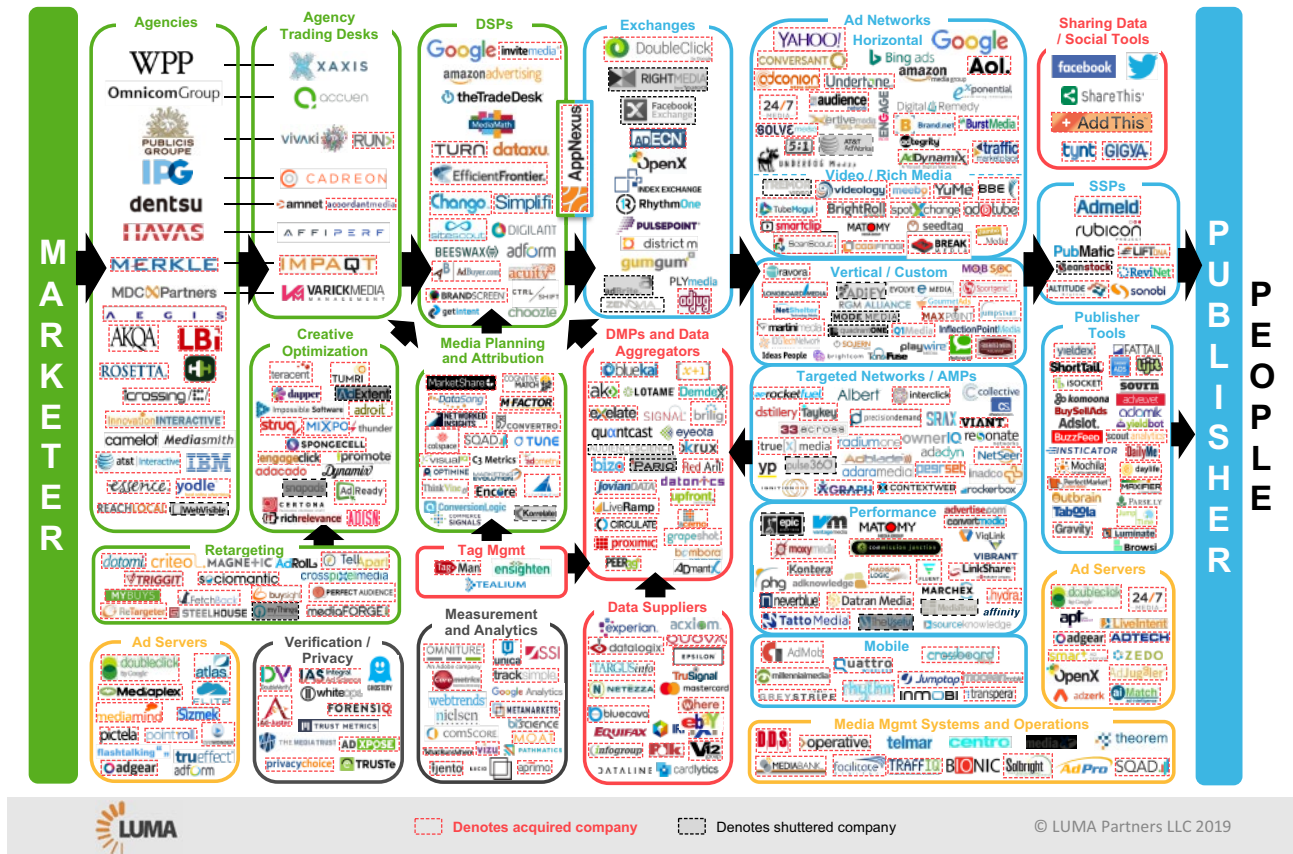
An opaque ad-tech ecosystem capitalises on the gold rush. Ad-tech companies have proliferated in the last seven years – in a space where very few existed just a decade ago. In 2011 there were slightly more than 1,200 ad-tech companies;⁴⁷ today, there are more than 5,000. The bewildering array of companies operating in this space is captured by what is known in the industry as the LUMAscape (see Figure 3). The companies involved range from those demanding and supplying headline banner space on pages to those serving as exchanges to connect these buyers and sellers – while collecting, aggregating, packaging, selling, and auditing all of the relevant data in between.

Since 2010, significant venture capital has flown into ad-tech to support the development of tools that were intended to make it easier for ad companies to target

and maintain customer relationships. Venture funds in ad-tech topped US\$7.2 billion in 2018, but this may drop by 75 percent in 2019.⁴⁸ The reason for this is expected consolidations: recent estimates suggest that the top 15 ad-tech companies alone control about 40 percent of the market – with the rest spread among small and niche vendors.⁴⁹

And as with all gold rushes, fraud has run rampant. Ad fraud for companies advertising online and via mobile networks is now estimated to cost advertisers about US\$51 million each day. Fraud can take the form of ads placed on websites visited only by bots, or ads not shown at all or shown only below the ‘fold’ of the page. The World Federation of Advertisers expects ad fraud to surpass the trade in illicit drugs and cause US\$50 billion in annual losses by 2025.⁵⁰

Figure 3: The LUMAScape of AdTech Players (Display)



Source: <https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/>

TREND 4:

Microtargeting and programmatic ads have made advertising more automated, precise and scalable.

With online ad spend booming, there has been a rise in the automatic placement of ads, or ‘programmatic’ ad networks. Programmatic ad spend is estimated to reach two-thirds of the total digital online ad spend by 2020.⁵¹ Hundreds of billions of dollars in online ad requests are bid for every day.⁵² The move to microtargeting these ads is fuelled by very precise behavioural and personal data that are continuously gleaned from each of us every time we use the internet – be it to read a news story, click on a post or buy something online. These data reveal what we buy, search for, like and share. It is estimated that one social media platform uses 52,000 personal attributes to classify people (based on their

interests and attributes).⁵³ As more information on us is gathered, this information can be used by advertisers to better target their ads to online users in real time. Every time you load a website, an automated advertising auction called a header bid takes place.⁵⁴ Based on one estimate, each bidding process takes 150 milliseconds to complete.⁵⁵ The impact of this automated process has been to remove human decision-making about where an advert gets placed. This opens up the risk that ads can land next to inappropriate content, and may ultimately compromise brand safety when one’s brand is automatically placed next to objectionable content of one form or another.

A system abused:

The money and the messages of disinformation

The ad-tech ecosystem is the perfect vehicle for targeting any type of message – not just which shampoo to buy or car to drive.

The system can be abused to spread messages that disinform, affecting our beliefs, ideas and actions.

At GDI we have identified the channels that are used to deliver such targeted messaging. We call this the precision messaging system (PMS). It is based on four interconnected parts of a cycle (see Figure 4):



STAGE 1: DISTRIBUTION

At this first stage, advertisers and disinformation actors alike can use similar distribution tools and channels to target a message to a specific group or individuals (using tools like ‘lookalike’ audiences to specify recipients and expand reach).

- For a sportswear brand, this might mean targeting all 15–24-year-old males living in middle-class Johannesburg neighbourhoods to ‘buy my sneakers’. For a disinformation actor it might mean targeting this same group to ‘buy into my immigration conspiracy’.



STAGE 2: BEHAVIOURAL RESPONSE

Individuals or groups receive this message or advert (which can include memes, video content, graphics, etc.) and they act, react, and/or amplify it.

- In this case the target group may now share the sportswear ad’s video clip which appears in their online feed (after their recent visit to a sneaker site). A conspiracy site may want to get the same target group to share via their own networks a manipulated video about immigrants attacking people.



STAGE 3: CONSUMER DATA

These actions and reactions are then captured by a person’s online data footprint on domains and platforms (where people buy, read, like, and engage with content).

- Increased data about this group of consumers can be gleaned, such as their political affiliation, ethnic background, income, and education level.



STAGE 4: CONTENT CREATION

This constantly updated and 'enhanced' footprint is then further used to refine how content or adverts are tailored to the user.

- For example, if an advertiser captures data showing that 15–24-year-old men in Johannesburg are more likely to buy sneakers on Friday nights, ads can be targeted for that time slot. Equally, if a disinformation actor knows that this same group also responds to anti-immigration messaging, they can be targeted at the same time with related conspiracy theories (which may even look like real news stories).

Figure 4: The Precision Messaging System



Source: Model developed by GDI

After the fourth stage, once the system has been fed more specific and detailed information about what consumers want, the cycle begins anew with the distribution of more specifically-tailored messaging to a user.

Every interaction we make online generates these insights about our behaviour, making the system ever more efficient at messaging – not only for commercial companies, but for disinformation actors as well.⁵⁶

What started out as an industry to help advertisers reach their customers ever more efficiently has become the most complete, effective and scalable behavioural modification system humans have ever invented.

The precision messaging system is effective at delivering disinformation because it taps into some fundamental human psychology (see below). We are attracted to ‘drama’ even more than pictures of cute kittens.⁵⁷ In an internet world, attention is finite and the demands on it are infinite. This means that only the content which calls loudest will get our attention. In the case of YouTube’s content moderation, critics have claimed that their formula is ‘outrage equals attention’ in order to increase engagement and ad revenues.⁵⁸ It is not surprising that over the lifetime of the internet, negative content which evokes our fear, hatred or disgust has propagated faster and farther than the cute kitten photos. One study of Twitter using a sampling of 126,000 rumours, showed that falsehoods were 70 percent more likely to be retweeted on Twitter than the truth.⁵⁹

Biased from the core: The ‘attention economy’ and polarisation⁶⁰

Technology taps into the same biases humans have always had, making us uniquely vulnerable to targeted disinformation messages. Here are some of the psychological biases that can feed the disinformation machine:

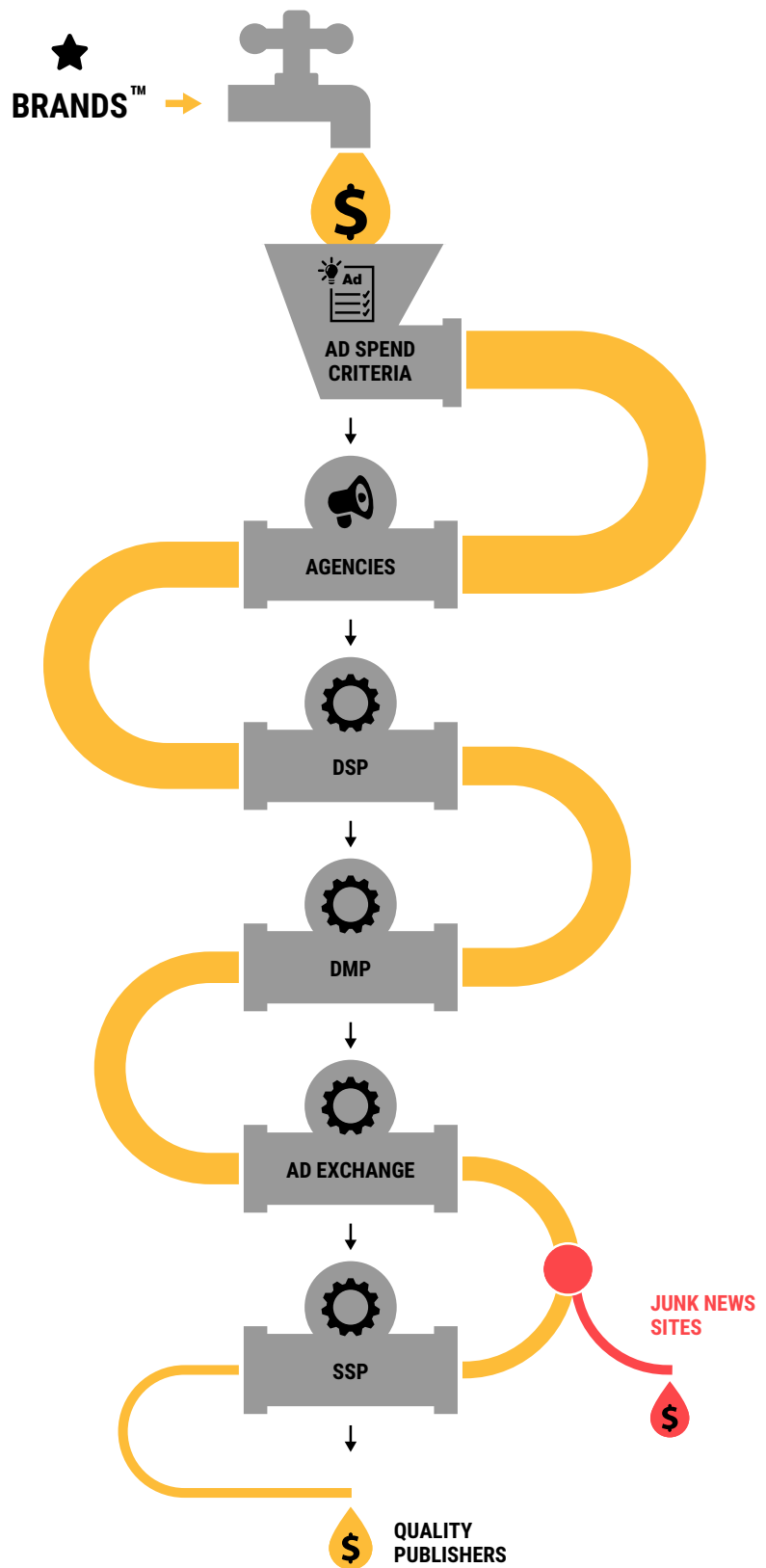
- **Bias blind spot:**⁶¹ This refers to the common tendency for people to notice all of the flaws in an opponent’s argument while failing to recognise any of their own – which explains why nobody thinks they’re biased. When we’re faced with the task of deciding whether a piece of information is true, the bias blind spot kicks in.
- **Declinism:**⁶² The belief that a society or institution is tending towards decline. This is why slogans like ‘Make America Great Again’ and ‘Take Back Control’ have been such effective messages for both the Trump campaign and Brexit. It is also why scapegoat groups are often blamed for a society’s decline.
- **Confirmation bias:**⁶³ Common across all forms of social media, this refers to people’s tendency to search for or interpret information in a way that confirms their pre-existing views. This is one major reason why people are more likely to click on disinformation headlines that reinforce their views, and why algorithms tend to turbocharge this bias.
- **Bandwagon effect:**⁶⁴ Also known as ‘herd mentality’, the bandwagon effect is the tendency to believe something is true or good, just because many other people believe it to be so. This can help disinformation purveyors spread their messages by ensuring they have enough likes or retweets, even if bots drive the traffic.
- **False consensus effect:**⁶⁵ People have a tendency to overestimate the extent to which the majority of others share their views. Social media heightens the false consensus effect because of algorithms that keep serving us content that matches our existing views.

Equally, domains that disinform are more likely than domains that inform to capture ad revenues, as they are more likely to engage users (due to their focus on negative emotions and being generally unconstrained by truth or reality). Everyone in the chain makes money – except, often, the high-quality news domains. The result is that low-quality online outlets are siphoning ad money away from quality ones and the audiences they attract (see Figure 5).⁶⁶ (Currently there are no reliable estimates of the size of the disinformation market in terms of the ad dollars and merchandise that support it. A forthcoming GDI paper will present a first attempt).⁶⁷

Over the last few years the proportion of ad spend reaching the end publisher has dwindled as a growing number of intermediaries have taken a cut: Demand Side Platforms (DSPs), Data Management Platforms (DMPs), Supply Side Platforms (SSPs), exchanges, and others. And with the advent of disinformation, this small trickle at the end of the pipe is now split further between quality and junk sites. It is estimated that online news publishers see about 40 percent of the ad spend from brands, and this number drops to as low as 28 percent when the estimate assumes that some money is lost to ad fraud. The rest is forgone to the ‘tech tax’ that is collected by different players along the way.⁶⁸

All of this reveals a crowded and opaque ad-tech ecosystem which has created opportunities for fraud and incentives for junky disinformation merchants to chase after eyeballs and ad monies. The result is that there has been – and will continue to be – a sharp drop in revenue to quality news publishers. Not only has the increase in disinformation overwhelmed the spread of high-quality information, it has also made quality journalism less financially viable.

FIGURE 5:



Source: Model developed by GDI

For the GDI, the abuse of the ad-tech system is at the heart of the problem of monetising and spreading the messages of disinformation. Here is one way that a disinformation actor might exploit the ad-tech ecosystem to spread its messages and generate money:

STEP 1:

An actor sets up a domain or uses an existing one to upload content that will grab the user's attention. Usually, the content is designed to appeal to emotions or biases, and often is gamed so as not to directly violate any community standards. For example, the actor might claim that the site is satire when it is not. The actor might even test samples of the content on various alternative platforms to measure how engaging they are among its target audience.

STEP 2:

Using the Precision Messaging System, the actor might target a link to the site or a sample of the content to attract visitors, for example, by sharing it in a group or paying to promote it to a custom audience on a social media platform.

STEP 3:

As the site gains visitors and is shared organically among its target audience, it is naturally promoted by platforms and search engines that reward 'engaging' content. The actor may also create inorganic engagement using bots that like, share, or otherwise engage with links to the site. This drives even more traffic to the site, and ultimately creates an air of legitimacy, often gaining the site recognition by more mainstream media.

STEP 4:

As more users, real or fake, visit the site and engage with its ads, the disinformation actor watches the money flow in. And if the actor is pushing a political agenda, it sees the disinformation campaign work.

STEP 5:

For every user who engages with this content, the various ad-tech platforms along the way – from the social media sites where the domain is being shared, to the ad exchanges that are brokering the banner ads – also gain revenue from this activity. And these users, along with the revenue that they bring, are diverted from the other publishers competing for their attention.

CASE STUDY

Building Disinformation Networks: Johann Fakra and his French empire

Journalists from *Le Monde* have found that one Frenchman, Johann Fakra, is allegedly behind a constellation of about 30 French-language websites known for reported disinformation efforts linked to conspiracies, far-right content, and dubious health information. This network is one of the biggest in France, and has spread claims that the Charlie Hebdo attacks were an inside job, and that garlic is 15 times more efficient than antibiotics at curing infections. His network was spotted because these websites, all of which also have Facebook pages, are all linked to the same Google AdSense and Google Analytics account. Some of the sites also used similar graphics and content.

In total, Fakra's Facebook pages for all of his sites amassed around 1 million engagements per month. This network has also been reportedly connected with other well-known disinformation actors in France⁶⁹ and the US.⁷⁰

Journalists have studied his sites and have found ads, mostly from Google or Taboola. The screenshot below, for example, shows a banner ad for Opel that appeared on one of the now deleted websites of this network, www.see-life.fr⁷¹ While the headline may arguably be true ('A 400-million-euro bug at France's employment agency'), the website itself has been flagged numerous times for publishing disinformation.



The GDI method

At the GDI, we see protecting the ad-tech ecosystem from abuse as part of the solution to combat efforts to disinform.

As an index, the GDI looks at content and context flags which can help to assess any domain's risk of disinformation. The GDI does not attempt to determine truth or falsehood. It aims to describe the risk of a domain disinforming its readers.

The GDI is working to develop a set of 'indicators' that can identify, measure and validate the risk of disinformation at the domain level. This set is based on:

- an automated, machine-learning assessment that can classify large volumes of low production quality 'junk' sites in real time; and
- a manual assessment of higher-quality disinformation outlets that may not be easily discernible by automated technical means.

The GDI plans to assess any domain that presents itself on the surface level as some form of news. GDI-assessed sites that are found to be risky may include high-volume purveyors of junk news, high-volume clickbait sites, and media outlets (either state-owned or commercial) which present themselves as journalism. The index will eventually cover all countries and major languages.

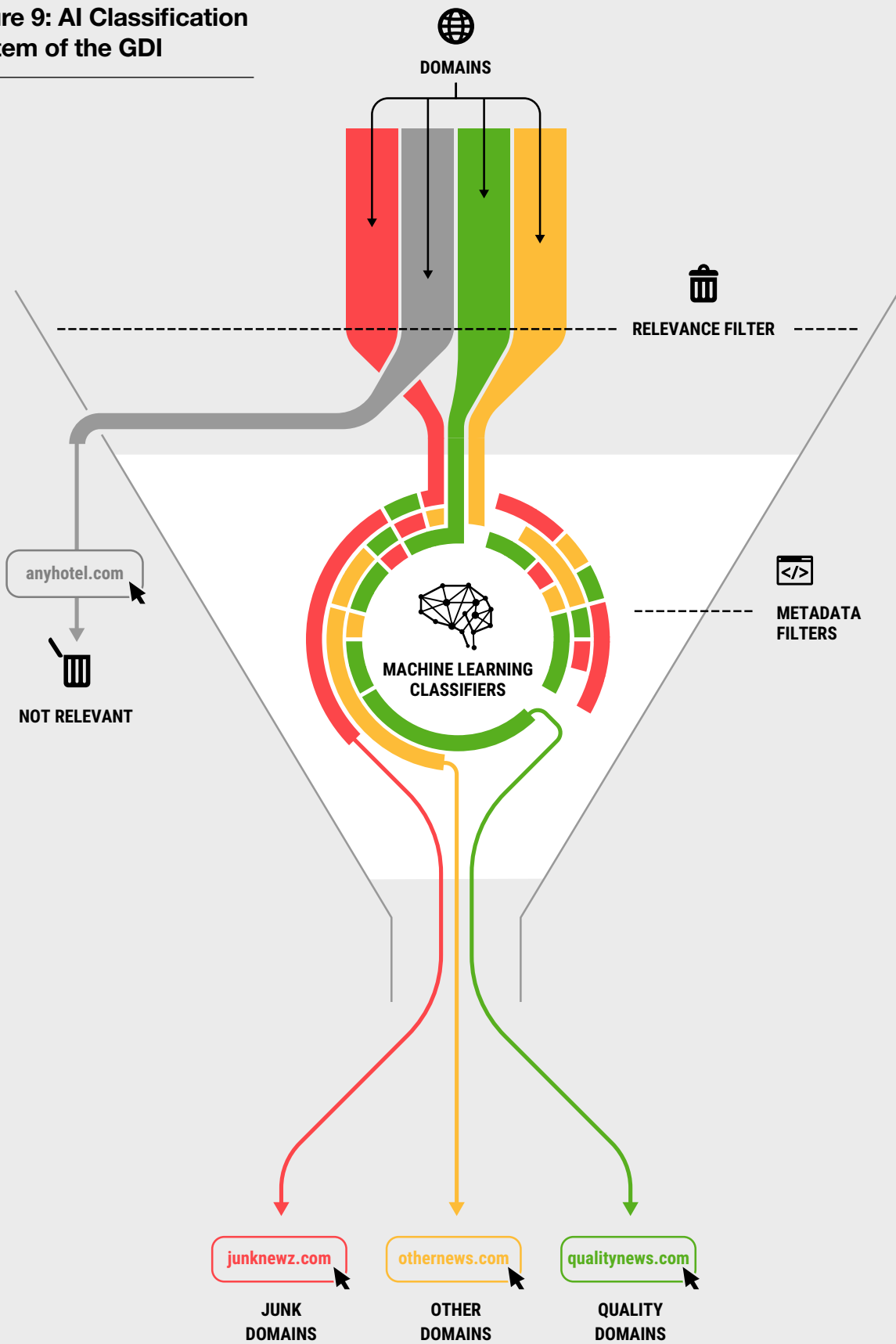
Automated assessment

The automated assessment focuses on technical metadata and other computational signals as proxy indicators of the quality of an online outlet. These are used to score whether a domain can be classified as presenting a high risk of disinforming, and whether it has seemingly been set up to generate clicks to gain ad monies: i.e. 'junk'.

The GDI's work in creating automated classifiers to capture 'junk' news sites builds on initial experiments performed in 2018 under a grant from the Knight Foundation Prototype Fund. In this demonstration, we trained a neural network classifier on hundreds of pre-labelled junk and quality news outlets, focusing on over twenty different technical metadata signals, including:

- Does the site employ HTTPS?
- Does the site use a subdomain?
- Does the registration email in the whois info match the domain?
- Does the site run PHP?
- Does the site have an ads.txt file?

Figure 9: AI Classification System of the GDI



Source: Model developed by GDI

We then tested the classifier's performance on more than 350 pre-labelled junk and quality news domains.⁷² The prototype classifier correctly identified 98.8 percent of the domains that had been pre-labelled as junk.⁷³ This prototype demonstrates the power of metadata to discern whether a site has been hastily assembled to capture ad revenue, or whether it represents a long-term investment by its operator.

The classifier can be imagined as a large funnel, consisting of a series of increasingly specific filters (see Figure 9). At each point, the filters classify each domain by using machine-learning algorithms to answer a series of yes/no questions about metadata indicators (as noted above).

Going forward, the GDI will look at other computational signals of content and metadata that can be used to further filter domains and automatically classify them as 'junk'.

These could include the following:

- Usage of hyperbolic or charged words;
- Cluster analysis of text content to detect text reuse across multiple sites;
- Language vocabulary level;
- Sentence complexity; and
- Token reuse (for example, for tracking services or ad providers) across multiple sites.

While this will help us keep pace with the speed at which sites in this category are created, we don't expect these signals to be effective in detecting more organised or professional actors who make long-term investments in their media outlets and engage in more pernicious forms of disinformation beyond clickbait. For this reason, we intend to manually review those news sites which are not scored as 'junk'.

Manual assessment

The manual process will be used for news domains that are not classified as 'junk' by the GDI's automated processes. These sites would be sorted into the 'other domains' and 'quality domains' baskets once they are passed through the filter.⁷⁴ We expect these sorts of domains to number between twenty and one hundred for any given media market.

The manual assessment will use proxy measures to assess these domains' risk of disinforming. The GDI is currently looking at different methodological options for conducting this assessment.⁷⁵

The manual assessment will include a set of discrete indicators that can help to flag the risk of a news domain to disinform. These indicators are to be based on the existing body of work advanced through initiatives such as the Trust Project and the Journalism Trust Initiative.⁷⁶ Indicators under consideration include such questions as whether the domain has had past involvement in disinformation campaigns, how many times it has been fact-checked, and whether the domain has issued corrections, among others.

Once the manual assessment has been conducted, the GDI will score news domains based on the results of the survey. These scores would be added to the findings from the automated assessment to produce a consolidated domain-level risk assessment (i.e. 'score').

The aim of the index assessment is to make sure that brands, advertisers and platforms have transparent and constant information about the domains on which they are buying ads and promoting, a sort of real-time list to replace the manually updated lists currently available. This information would be automatically fed into different decision-making points in the ad-tech ecosystem (Figure 10):

1. AD-SPEND CRITERIA:

- Lists of GDI-rated domains are automatically shared with brand owners.
- Brands incorporate ratings and domains lists into their ad-spend criteria, campaign plans, and brand-safety objectives. (see Figure 10, 'Ad-Spend Criteria').
- Brands direct ad spend to domains that score above a specified GDI rating.

2. AD EXCHANGES:

- Ad exchanges link up with real-time feed from GDI-rated 'junk' domains.
- Ad exchanges use the feed to set criteria for domains that can use their exchange to bid out space for online ads.
- Ad exchanges are protected from legal risks and provide brand safety to their customers. (see Figure 10, 'Ad Exchange').

3. PLATFORM RECOMMENDATIONS:

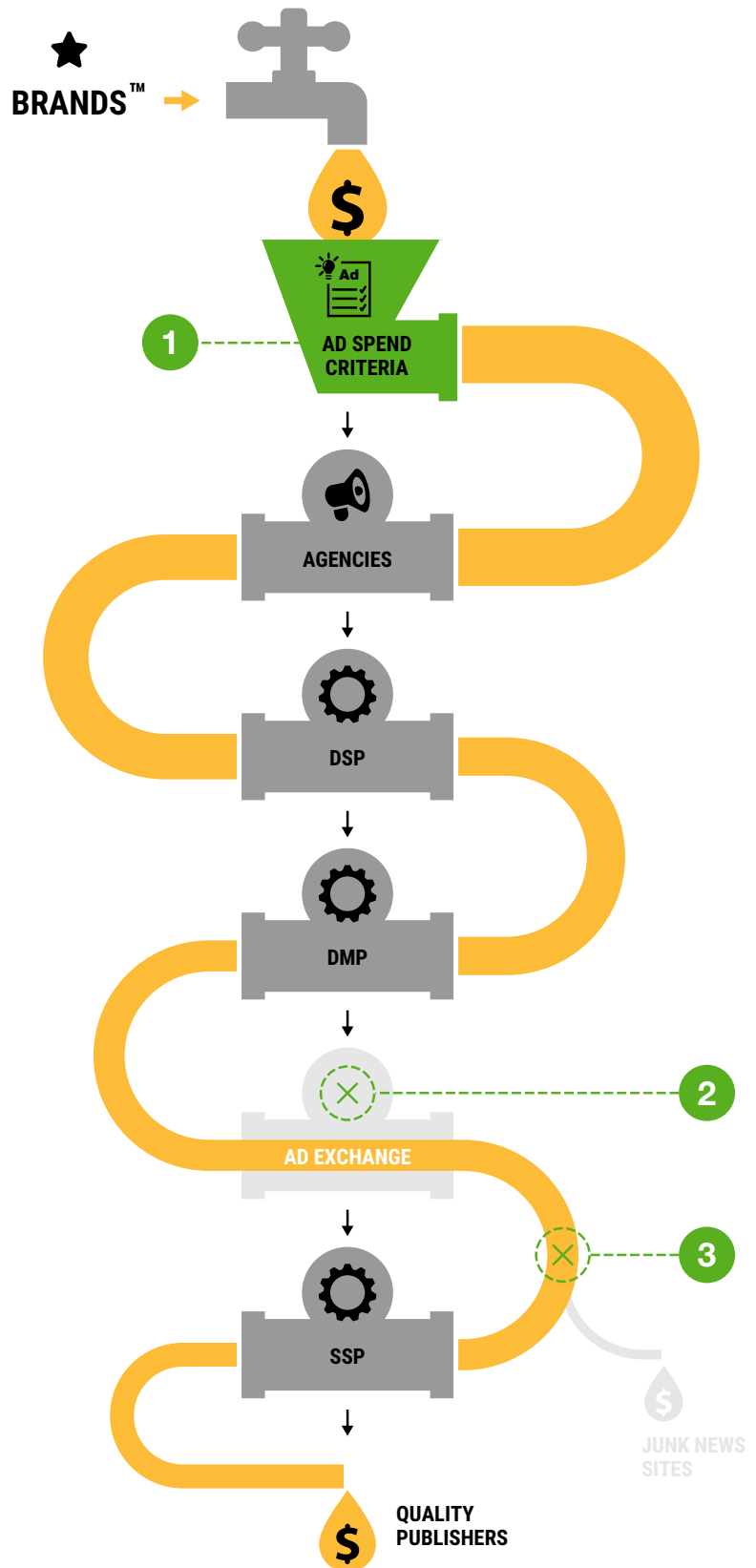
- The GDI provides to platforms overall index ratings and a real-time feed of 'junk' domains.
- Platforms and search engines plug GDI ratings and list of junk domains into recommendation algorithms.
- Platforms use GDI ratings to set 'tolerance thresholds' for which domains to promote in feeds and searches.

The overall results from turning off the money tap will be to:

- cut off monies from online adverts on disinforming domains,
- strengthen the funding line from online ads to quality news domains,
- reduce disinformation by financially-motivated actors, and
- curtail the ability to amplify some of the messaging of politically-motivated actors.

Such a systemic approach is a necessary step in combating efforts to disinform. By early 2020, we plan to pilot this approach and the index in at least five English-language countries, working closely with brands, ad exchanges and platforms in the process.

Figure 10: Cleaning Up the System



Source: Model developed by GDI

The way forward

It is time for brands, advertisers, online media and platforms to recognise their role in the problem – and the solution.

Our online space has been hijacked by those seeking to disinform. We are reaching a tipping point where the web could lose its positive role as a platform for the free flow of information and ideas.

While efforts to disinform existed before the web, the social- and ad-driven internet represents an entirely new chapter in the history of disinformation. Unfortunately, the internet is being used by disinformation actors in order to profit from and amplify their messages. It is time to rethink the best approaches to protect the web from domains that disinform. The GDI is an attempt to contribute to the solution.

One key aspect of stopping disinformation is understanding how the online advertising system is being abused by those that disinform. A system that was designed for one purpose (to make advertising more efficient) is being abused for another (to disinform for financial and political ends). It is time for a systemic fix.

The GDI offers this approach. It provides for real-time ratings on a domain's risks of disinforming that can be plugged in and used by brands, ad exchanges and platforms to cut off the funding flow to disinformation domains as well as to provide online users with needed information about their news sources.

With the GDI ratings:

- **Brands and media agencies** will have a better understanding and greater control over whether their advertisements are being placed on risky sites.
- **The ad-tech community** will have non-biased feedback to direct ad money away from domains with high disinformation risks.
- **Social platforms and search engines** will have neutral ways to encourage the spread of information and rein in disinformation efforts.
- **Online users** will have greater context about the domains which they read, comment on, and share.

The GDI is a collaborative and effective way to stop the disinformation damage to our societies, economies and politics. Working together is the only way to tackle this challenge.

It is time for brands, advertisers, online media and platforms to recognise their role in the problem – and the solution.

Endnotes

- 1 This is defined by First Draft as: ‘false information that is deliberately created or disseminated with the express purpose to cause harm. Producers of disinformation typically have political, financial, psychological or social motivations.’ See: Wardle, C. (2018, July 9). Information disorder, part 1: The essential glossary. Retrieved from <https://medium.com/1st-draft/information-disorder-part-1-the-essential-glossary-19953c544fe3>. Note that this is different from ‘misinformation’, which is defined as ‘information that is false or misleading’. See: Zhang, A et al. (2018). A Structured Response to Misinformation: Defining and Annotating Credibility Indicators in News Articles. *WWW2018 Proceedings*. Retrieved from <https://credco.meedan.com/pdfs/CredCoWebConf2018.pdf>.
- 2 ‘The term ‘ad-tech’, which is short for advertising technology, broadly refers to different types of analytics and digital tools used in the context of advertising. Discussions about ad-tech often revolve around the extensive and complex systems used to direct advertising to individuals and specific target audiences through digital channels. See: Ad-tech. (n.d.). Retrieved from <https://www.techopedia.com/definition/31293/ad-tech>.
- 3 Moon Sehat, C. (2019, January 25). Kermit is credible, and this is good for news. Approaches to tackling misinformation for the year ahead. Retrieved from <https://misinfocon.com/kermit-is-credible-and-this-is-good-for-news-f26f595a356e>.
- 4 For example, please see: Nyabola, N. (2018, November 5). Fake news is not just a Western problem. Retrieved from <https://newint.org/features/2018/11/01/fake-news-africa>; Noah Harari, Y. (2018, August 5). Yuval Noah Harari extract: ‘Humans are a post-truth species’. Retrieved from <https://www.theguardian.com/culture/2018/aug/05/yuval-noah-harari-extract-fake-news-sapiens-homo-deus>; and Inside the Russian disinformation playbook: Exploit tension, sow chaos. (2018, November 15). Retrieved from <https://www.npr.org/2018/11/15/668209008/inside-the-russian-disinformation-playbook-exploit-tension-sow-chaos>.
- 5 Berg, S. (2019, March 18). ‘Fake news’ sent out by government department. Retrieved from <https://www.bbc.com/news/uk-politics-47571253>.
- 6 The US government reportedly used information propaganda and disinformation tactics during and after the war in Iraq. See: Barstow, D. (2008, April 20). Behind TV analysts, Pentagon’s hidden hand. Retrieved from <https://www.nytimes.com/2008/04/20/us/20generals.html> and Greene, R. (2011, March 2). Military may be engaged in illegal psychological operations and propaganda against U.S. citizens. Retrieved from <https://www.aclu.org/blog/free-speech/employee-speech-and-whistle-blowers/military-may-be-engaged-illegal-psychological>.
- 7 A good overview was collected of some alleged actions between 2010 and 2017. See p. 13: Bradshaw, S and Howard, P. (2017). *Troops, trolls and troublemakers: A global inventory of organized social media manipulation*. Retrieved from <https://comp-op.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>.

- 8 Lau, J. (2016, October 7). Who are the Chinese trolls of the '50 Cent Army'?. Retrieved from <https://www.voanews.com/a/who-is-that-chinese-troll/3540663.html>.
- 9 Corpus Ong, J and Cabanes, J. (2018, February 11). Chief disinformation architects in the PH: Not exactly who you think. Retrieved from <https://www.rappler.com/thought-leaders/195743-disinformation-architects-philippines>.
- 10 Suspected Iranian influence operation leverages network of inauthentic news sites & social media targeting audiences in U.S., UK, Latin America, Middle East. (2018, August 21). Retrieved from <https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html> and Removing coordinated inauthentic behavior from Iran. (2019, January 31). Retrieved from <https://newsroom.fb.com/news/2019/01/removing-cib-iran/>.
- 11 The strategy and tactics of the pro-Kremlin disinformation campaign. (2018, June 27). Retrieved from <https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/>.
- 12 The Guptas, Bell Pottinger and the fake news propaganda machine. (2017, September 4). Retrieved from <https://www.timeslive.co.za/news/south-africa/2017-09-04-the-guptas-bell-pottinger-and-the-fake-news-propaganda-machine/>.
- 13 Roth, Y. (2019, January 31). Empowering further research of potential information operations. Retrieved from https://blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html.
- 14 Removing coordinated inauthentic behaviour from Iran, Russia, Macedonia and Kosovo. (2019, March 26). Retrieved from <https://newsroom.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/>.
- 15 Gobierno de México denuncia campaña financiada supuestamente por la firma OHL. (2019, March 4). Retrieved from <https://www.efe.com/efe/usa/mexico/gobierno-de-mexico-denuncia-campana-financiada-supuestamente-por-la-firma-ohl/50000100-3924883>.
- 16 Chaudhuri, P. (2019, March 2). Dangerous, manufactured audio clip used to claim Pulwama terror attack an inside job by BJP. Retrieved from <https://www.altnews.in/dangerous-manufactured-audio-clip-used-to-claim-pulwama-terror-attack-an-inside-job-by-bjp/>.
- 17 For more on #pizzagate, see: Samuelson, K. (2016, December 5). What to know about pizzagate, the fake news story with real consequences. Retrieved from <http://time.com/4590255/pizzagate-fake-news-what-to-know/>. For more on #gamergate, see: <https://www.theguardian.com/games/gamergate>.
- 18 Ha, A. (2019, February 26). Rotten Tomatoes tries to combat trolls with audience rating changes. Retrieved from <https://techcrunch.com/2019/02/26/rotten-tomatoes-trolls/>.
- 19 Mezzofiore, M. (2018, November 1). They were the only all-female, all-black team in a NASA science competition. Then came the hackers. Retrieved from <https://edition.cnn.com/2018/05/03/us/black-teens-nasa-science-competition-4chan-hackers-trnd/index.html>.
- 20 Ad arbitrage refers to when the an actor buys ads promoting their domain while selling ads on the same domain at different prices to turn a profit.
- 21 O'Sullivan, D. (2018, October 18). Exclusive: Women's March target of elaborate Facebook scam run from Bangladesh. Retrieved from <https://edition.cnn.com/2018/10/17/tech/womens-march-facebook-scam-bangladesh/index.html>.

22 Miller, C. (2018, September 7). The dangerous powers of the clickbait king. Retrieved from <https://kosovotwopointzero.com/en/the-dangerous-powers-of-the-click-bait-king/>.

23 Fay, J. (2018, August 20). The death of the gods: Not scared of tech yet? You haven't been paying attention. Retrieved from www.theregister.co.uk/2018/08/20/book_review_the_death_of_the_gods_the_new_global_power_grab/.

24 See, for example, how a Russian parody article was reported as truth by Fox News after it was legitimised by Western tabloids and alternative news websites. DFRLab. (2017, March 9). Russia's fake 'electronic bomb': How a fake based on a parody spread to the Western mainstream. Retrieved from <https://medium.com/dfrlab/russia-fake-electronic-bomb-4ce9dbbc57f8>.

25 See, for example: <https://sherbrooktimes.com>, <https://qtelegram.com>, <https://sivtelegram.media>, <https://web.archive.org/web/20170626181130/http://vtabloid.com/>, and <https://sivertimes.com>.

26 As of 28 March 2019, the site was still active.

27 This was discovered by doing a reverse image search.

28 Community 'now living in fear' after reporter gets it wrong: Checkup caller. (2017, December 17). Retrieved from www.cbc.ca/radio/checkup/fake-news-how-do-you-ensure-the-news-you-get-is-trustworthy-1.4450145/community-now-living-in-fear-after-reporter-gets-it-wrong-checkup-caller-1.4454463.

29 Ibid.

30 *The Siver Times*, for example, has about 200,000 unique visitors a month.

31 Who you gonna trust? Newspapers! (2018, November 14). Retrieved from <https://nmc-mic.ca/news/research/who-you-gonna-trust-newspapers/>.

32 Kasprak, A. and Palma, B. (2019, March 4), Hiding in plain sight: PAC-connected activists set up 'local news' outlets. Retrieved from <https://www.snopes.com/news/2019/03/04/activists-setup-local-news-sites/>.

33 Cooper, P. (2019, January 16). 28 Twitter statistics all marketers need to know in 2019. Retrieved from <https://blog.hootsuite.com/twitter-statistics/>.

34 This was calculated from the metric of 4 million Facebook posts being liked every minute. See: Carey-Simos, G. (2015, August 19). How much data is generated every minute on social media?. Retrieved from <https://wersm.com/how-much-data-is-generated-every-minute-on-social-media/>.

35 Newman, N. (2017). *Reuters Institute digital news report 2017*. Retrieved from https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf.

36 Ibid.

37 Ibid.

38 Eva Matsa, K and Shearer, E. (2018, September 10). News use across social media platforms 2018. Retrieved from <https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/>.

39 2019 Edelman Trust Barometer reveals 'My Employer' is the most trusted institution. (2019, January 20). Retrieved from www.edelman.com/news-awards/2019-edelman-trust-barometer-reveals-my-employer-most-trusted-institution.

40 Ibid.

41 Molla, R. (2018, March 26). Advertisers will spend \$40 billion more on internet ads than on TV ads this year. Retrieved from www.recode.net/2018/3/26/17163852/online-internet-advertisers-outspend-tv-ads-advertisers-social-video-mobile-40-billion-2018.

42 Zenith. (2018). *Global intelligence: Data & insights for the new age of communication*. Retrieved from https://www.zenithmedia.com/wp-content/uploads/2018/11/Global-Intelligence-07_small.pdf.

43 AppNexus. (2018). *The digital advertising stats you need for 2018*. Retrieved from https://www.appnexus.com/sites/default/files/whitepapers/guide-2018stats_2.pdf.

44 These are officially reported numbers. Third-party monitors estimated spending to be much higher. See Nicolai, A; Larraz, I; and González, O. (2018, June 4). Verificado. mx: Candidatos gastan más de 106 mdp en propaganda en internet, pero no declaran todos los anuncios. Retrieved from www.animalpolitico.com/2018/06/verificado-candidatos-anuncios-internet/.

45 Borrell. (2017, November 29). *2018 local political advertising outlook*. Retrieved from www.borrellassociates.com/industry-papers/papers/2018-local-political-advertising-outlook-detail and Janetsky, M. (2018, March 7). Low transparency, low regulation online political ads skyrocket. Retrieved from www.opensecrets.org/news/2018/03/low-transparency-low-regulation-online-political-ads-skyrocket/.

46 The UK Electoral Commission. (2018, June). *Digital campaigning: Increasing transparency for voters*. Retrieved from www.electoralcommission.org.uk/_data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf.

47 Johnson, L. (2018, March 1). When Procter & Gamble cut \$200 million in digital ad spend, it increased its reach 10%. Retrieved from <https://www.adweek.com/brand-marketing/when-procter-gamble-cut-200-million-in-digital-ad-spend-its-market-ing-became-10-more-effective/> and Efrati, A. (2011, July 6). Online ads: Where 1,240 companies fit in. Retrieved from <https://blogs.wsj.com/digits/2011/06/06/online-ads-where-1240-companies-fit-in/?mg=prod/accounts-wsj>.

48 Ives, N. (2018, November 5). Funding for start-ups in marketing, ad-tech is expected to fall in 2019, report says. Retrieved from <https://www.wsj.com/articles/funding-for-startups-in-marketing-ad-tech-is-expected-to-fall-in-2019-report-says-1541455170>.

49 Weide, K and Shirer, M. (2018, September 18). Worldwide ad-tech market still highly fragmented despite intense M&A activity, continuing strong growth spells opportunity, according to IDC. Retrieved from www.idc.com/getdoc.jsp?containerId=prUS44288518.

50 Handley, L. (2018, October 23). US and UK join up to tackle ad fraud, a \$50 billion problem. Retrieved from <https://www.cnbc.com/2018/10/23/us-and-uk-join-up-to-tackle-ad-fraud-a-50-billion-problem.html>.

51 Yieldbird. (2017). *2018 Global Programmatic Trends*. Retrieved from <https://yieldbird.com/wp-content/uploads/2017/12/Global-Programmatic-Trends-2018-by-Yieldbird.pdf>.

52 These figures are based on a presentation by Dr. Johnny Ryan, Chief of Policy for Brave: Ryan, J. (2019, February 14). *The adtech crisis and disinformation*. Retrieved from <https://vimeo.com/317245633>.

- 53 See p. 8: European Data Protection Supervisor. (2018). EDPS Opinion on online manipulation and personal data. Retrieved from https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
- 54 Bilton, R. (2015, August 18). WTF is header bidding?. Retrieved from <https://digi-day.com/media/wtf-header-bidding/>.
- 55 Adshead, S; Forsyth, G; Wood, S; & Wilkinson, L. (2019, January). Online advertising in the UK. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777996/Plum_DCMS_Online_Advertising_in_the_UK.pdf.
- 56 The argument about behavioural data and its use for systems of disinformation was noted in Ghosh, D and Scott, B. (2018). Retrieved from <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/>.
- 57 Fisher, N. (2018, August 10). Your brain on drama: What social media means for your personal growth. Retrieved from <https://www.forbes.com/sites/nicolefisher/2018/08/10/your-brain-on-drama-what-your-social-media-means-for-personal-growth/#2fd7b9307e91>.
- 58 Bergen, M. (2019, April 2). YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant. Retrieved from www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant.
- 59 These data are based on the period from 2006–2017. News was classified as true or false using information from six independent fact-checking organizations that exhibited 95 to 98 % agreement on the classifications. ‘Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information.’ See: Vosoughi, S; Roy, D & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151.
- 60 This text was prepared by Samantha North of the GDI.
- 61 Pronin, E; Lin, DY; & Ross, L. (2002). The Bias Blind Spot: Perceptions of Bias in Self Versus Others. *Personality and Social Psychology Bulletin*, 28(3), 369–381. <https://doi.org/10.1177/0146167202286008>.
- 62 Gopnik, A. (2011, September 12). ‘Decline, Fall, Rinse, Repeat’. *The New Yorker*. Retrieved 04 April 2019 from <https://www.newyorker.com/magazine/2011/09/12/decline-fall-rinse-repeat>.
- 63 Lord, CG; Ross, L; Lepper, MR. (1979), ‘Biased assimilation and attitude polarization: The effects of prior theories on subsequently considered evidence’, *Journal of Personality and Social Psychology*, 37 (11): 2098–09, CiteSeerX [10.1.1.372.1743](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.372.1743), doi:10.1037/0022-3514.37.11.2098, ISSN 0022-3514.
- 64 Swann, WB; Read, SJ. (1981), ‘Acquiring Self-Knowledge: The Search for Feedback That Fits’, *Journal of Personality and Social Psychology*, 41 (6): 1119–28, CiteSeerX [10.1.1.537.2324](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.537.2324), doi:10.1037/0022-3514.41.6.1119, ISSN 0022-3514.
- 65 Ross, L; Greene, D; House, P. (1977) The ‘false consensus effect’: An egocentric bias in social perception and attribution processes, *Journal of Experimental Social Psychology*, Volume 13, Issue 3, pp 279–301.

66 Some analysis has argued that as users are now served up ads that are based on their personal data wherever they go, this problem includes questionable sites. In turn, the quality of online outlet audiences is being devalued. See: Ryan, J. (2019, February 1). The adtech crisis and disinformation. Retrieved from <https://www.slideshare.net/JohnnyRyan/the-adtech-crisis-and-disinformation>.

67 Williamson, E & Steel, E. (2018, September 7). Conspiracy theories made Alex Jones very rich. They may bring him down. Retrieved from <https://www.nytimes.com/2018/09/07/us/politics/alex-jones-business-infowars-conspiracy.html>.

68 Automation vs waste: the programmatic conundrum. (2018, March 29). Retrieved from https://www.warc.com/newsandopinion/news/automation_vs_waste_the_programmatic_conundrum/40252.

69 Sénécat, A. (2018, November 13). ‘« Ça doit se savoir », « Alter Santé », « Libre Info » : un seul homme derrière un réseau de désinformation. Retrieved from https://www.lemonde.fr/les-decodeurs/article/2018/11/13/ca-doit-se-savoir-alter-sante-libre-info-un-seul-homme-derriere-un-reseau-de-desinformation_5382951_4355770.html.

70 Evon, D. (2017, June 7). Did Trump Tour a Chemtrail Plane? Retrieved from <https://www.snopes.com/fact-check/trump-tour-chemtrail-plane/>.

71 Sénécat, A. (2018, November 13). « Ça doit se savoir », « Alter Santé », « Libre Info » : un seul homme derrière un réseau de désinformation. Retrieved from https://www.lemonde.fr/les-decodeurs/article/2018/11/13/ca-doit-se-savoir-alter-sante-libre-info-un-seul-homme-derriere-un-reseau-de-desinformation_5382951_4355770.html.

72 These were supplied from sources such as PolitiFact, Opensources.co, and Signal Media.

73 This was based on a list of nearly 2,000 domains which were assessed and had already been classified as known ‘junk’ or ‘quality news’ domains.

74 The expectation is to classify all domains on the web into four baskets: not relevant (not news-related domains), junk news, quality news, and other news domains (having some traits of quality and junk-news domains).

75 A scoping paper with potential methodologies for indicators and data collection methods will be made public for comment on the GDI website in May 2019.

76 RSF and its partners unveil the Journalism Trust Initiative to combat Disinformation. (2018, April 3). Retrieved from <https://rsf.org/en/news/rsf-and-its-partners-unveil-journalism-trust-initiative-combat-disinformation>. Also see <https://thetrustproject.org/>.



www.disinformationindex.org