Written Representation 102

Name: Kriel.Agency

Received: 2 Mar 2018

Summary	Fake news is now one of the most powerful forces countering democracy. It undermines the public's faith in democratic institutions operating in the context of the civil society, and inspires radicalisation and extremism within communities. Online propaganda has grown exponentially with the rise of social media, and at its most effective employs software automation processes, or bots, to both create disinformation content and distribute propaganda in highly targeted ways. It also does so through behavioural science techniques, data analytics, and addressable advertising technology.
Phenomenon of using digital technology to deliberately spread falsehoods online	Executive Summary Fake news is misleading online news and disinformation, also known as computational propaganda. Fake news is now one of the most powerful forces countering democracy. It undermines the public's faith in democratic institutions operating in the context of the civil society, and inspires radicalisation and extremism within communities. Online propaganda has grown exponentially with the rise of social media, and at its most effective employs software automation processes, or bots, to both create disinformation content and distribute propaganda in highly targeted ways. It also does so through behavioural science techniques, data analytics, and addressable advertising technology.

The rise of social media changed the nature and distribution of real news — the product of the news room is no longer a newspaper or news programme, but rather a collection of packages of information about a subject that can then be exchanged between readers on social media according to their interests. In this viral environment, the most sensational story survives and thrives. This creates an ecosystem overpopulated with wildly exaggerated or completely fabricated stories — an ecosystem easily exploited by malevolent agents. Software and social media make it possible for this exploitation to take place at scale.

We recommend:
Resisting legislation that might inadvertently compromise freedom of speech and access to information.

Establishing programmes to promote critical thinking skills around digital and social media.

Making software tools available to civil society organisations allowing them to measure the impact of their counter-narrative programmes on communities.

Increasing government spending on capacity development for civil society organisations engaged in counter-narrative programmes in the context of countering extremism.

Understanding that constant vigilance and long-view approaches backed by ongoing programmes of media education and literacy are vital to maintaining the interests and ideals of civil society and democracy.

What is fake news?
Fake news is a contentious term referring to packages of

misleading online news and disinformation; it is also often called influence campaigning or, when driven by social media and websites, computational propaganda.

Due to the nature of the Internet, fake news is international by default, with few boundaries save language. The recent US elections drew the world's attention to this new social media phenomenon. But the roots of fake news and propaganda run deep.

Contemporary fake news is much more than just disinformation deployed on a Facebook wall. It uses a combination of digital and human tools — algorithms, automated processes and human selection — to distribute highly targeted disinformation over social media networks.

Deployed at scale, bots, or automated scripts that create and distribute Tweets and Facebook posts, are capable of flooding channels and dominating public discourse.

Influence and political campaigns frequently employ algorithms to generate tens of thousands of web pages designed to persuade individuals targeted through typological profiling based on their online footprints, aggregating data from Facebook, Twitter and publicly available demographic information. Automation directs bespoke messaging at individuals based on what is most likely to persuade them. Although these are mass disinformation campaigns, individuals can still be targeted based on their consumer habits and demographic data, as well as their likes, dislikes and fears. The granular customisation of targeted disinformation spans the use of language, design and messaging, and can be used not only to sway opinion, but to both encourage and discourage certain

behaviours, like turning up to vote or violent extremism.

The three pillars

The three technological pillars driving fake news to customised audiences through targeted distribution are: behavioural science; data analytics; and addressable advertising technology. Behavioural science is used to develop typological personality profiles of online readers and platform users. Data analytics are used to scan social media profiles to determine a user's biases and behaviours. And addressable advertising technology is utilised in micro-targeting users with persuasive messaging.

Behavioural science

Behavioural science employs typological personality profiling to define the personality of the target. Whereas older systems like Myers-Briggs divided audiences into sixteen personality types — Introverted / Sensing / Thinking / Judging for example — more contemporary five factor modelling systems like O.C.E.A.N. allow for thousands of individual personality types.

The five factors (O.C.E.A.N.) used to glean personality are:

Openness — inventive and curious vs. consistent and cautious

Conscientiousness — efficient and organised vs. easy-going and careless

Extraversion — outgoing and energetic vs. solitary and reserved

Agreeableness — friendly and compassionate vs. challenging and detached

Neuroticism — sensitive and nervous vs. secure and confident

These five domains contain most known personality types, and are frequently determined online through granular analysis of social media profiles combined with openly available demographic data.

Data analytics

Companies engaged in analytics and influence campaigns often employ natural language processing and link content to analyse a social media user's general sentiment regarding certain subjects. This is done with tools like IBM's Watson, and algorithms like those developed at Cambridge's Machine Learning Group. Even more useful, and particularly when analysing huge data sets with billions of data points, is the simple Facebook or Twitter "like", now expanded on Facebook to include like, love, haha, wow, sad and angry.

Influence campaign operators include companies like Cambridge Analytica and Spectra Analytics. These personality profiling data companies gain access to a user's data through enticements like online games and surveys that require registration through Facebook. The user can then take the survey, answering a few preference questions ("Which actor should play you in your biography?" for example), and the data analytics company is given access to the user's Facebook profile and history, which often runs into hundreds of pages. UK-based Cambridge Analytica and parent company SCL are notorious for allegedly tricking 30 million Facebook users out of their data through a scheme launched via Amazon Web Services. Online freelancers working through Amazon's Mechanical Turk portal were paid to complete surveys, but also had to give one of SCL's partner companies - Global Science Research - access to all of their Facebook data, and that of all their friends. This violated Amazon's terms of service, and the

company was quickly suspended, but not until data on 30 million users had been harvested.

Cambridge Analytica claims that with access to just ten of a user's likes, they are able to predict that user's behaviour better than a co-worker might. With 300 likes, they can do so better than the user's spouse. That same company claims in their own literature to hold over 5,000 data points on every adult in the United States — 220 million people — and it is thought they hold the same on much of the British population.

Addressable ad technology
Based on the results of their behavioural and personality analytics, practitioners of computational propaganda will then target each user with fake news, designed to create change — to inspire action, suppress behaviour (like voting), change opinion, or, as is rapidly being learned of many covert Russian operations in Western countries, undermine a citizen's faith in their democratic institutions.

The user is targeted with social medias post that contain highly customised misinformation designed for that user's personality type and previously expressed preferences. Dark posts are notoriously difficult to discover or regulate; by design they can only be seen by the targeted user. But the Guardian has reported extensively on the use of dark posts in UK elections.

The New York Times recently reported a stark U.S. example, when members of the Congressional Black Caucus wrote to Facebook CEO Mark Zuckerberg questioning how the platform allowed Russian operatives to place adverts sowing racial division, and specifically targeting Black Lives Matter supporters. "Russian groups backed by the country's president, Vladimir V. Putin, paid

	Facebook to influence voters last year by 'purchasing ads designed to inflame and exploit racial, political and economic rifts in the U.S.,'" they wrote, quoting Illinois Representative Robin Kelly. Kelly went on to say that Russian-backed Facebook pages promoted "incendiary anti-immigrant rallies, targeted the Black Lives Matter movement and focused attentions on critical election swing states like Wisconsin and Michigan." These kinds of posts typically go undocumented, as they are "dark posts". Facebook dark posts are highly targeted adverts that only the targeted user can see, and they are often used to spread fake news about critical issues.
Motivations and reasons for the spreading of such falsehoods	Undermining democracy and public faith in institutions is an essential tenet of hybrid warfare, whether practiced by foreign agents or home-grown extremists seeking to radicalise vulnerable citizens.
Consequences of online falsehoods on Singapore society	Impact and risks to society The professional news environment is rapidly changing in response to online distribution, social media and extraordinary economic pressure demanding a change in business models. The product of the news room has ceased to be a newspaper or a morning radio programme. It is now a discrete package of information to be used as a social token in the better interests of a community. One form might be a single article posted on Facebook to be shared amongst members of a community. That community could be a demographic group, a group of citizens, or a community of interest — the citizens of the UK, or an international community with a shared hobby. Fake news is similar, but with a critical difference. The product of the fake news operation is disinformation

designed for maximum virality within the community — misinformation created to be shared.

Angry people click and share more, and in the fake news eco-system, sensationalist propaganda is highly viral.

The dangers of the proliferation of fake news can most easily be demonstrated through the results of influence campaign operations in conflict zones and fragile, emerging democracies.

Ukraine has become a laboratory for social media manipulation, with both the West and Russia conducting Facebook and Twitter wars to influence the population. These campaigns work to destabilise the other side's social narrative, with operations at work in Ukraine, and in nearby Poland. In some places online public life is completely dominated by bots on social media. In others, rumour and conjecture — frequently seeded through highly designed propaganda — make their way onto mainstream news platforms.

Social media is overrun by automated bots and manual trolls, sponsored by governments and organised disinformation campaigns. The political sections of some platforms are dominated by propaganda operations, including bot-driven campaigns, comment-section-flooding of news sites, and the bullying of social media users into silence, stifling real debate and dominating the dialogue of public life.

In the UK EU Referendum, a recent academic study has shown that an array of Twitter bots operating across 13,493 accounts regularly tweeted pro-Leave messaging. Those bots and accounts disappeared the day after the vote. And executives from Twitter,

Facebook and Google all recently testified before US Congress that their platforms had been exploited by Russia to interfere in US politics.

Ukraine is the frontline for experimentation with and the development of online disinformation. Russian, Ukraine nationalist, and civil society botnets swarm Ukraine's public arena, dominate discourse in a flood of competing disinformation. It is open warfare of a radically new variety.

Looking to the examples of Russian operations to target both Black Lives Matter supporters in the United States and Russian Nationalists in Ukraine, it is obvious that fake news is also a powerful tool for online radicalisation, as well as destabilisation of democratic governments operating in the context of the civil society. Much of fake news is sensationalist by design, and built to both appeal to potential extremists, and to inflame emotions. As outlined earlier, angry people click more. And often they act on their new-found ideological views with violence.

As with the aftermath of the Las Vegas shootings, shortly after the Manchester Terror Attack at an Ariana Grande concert, social media was flooded with fake news about the attack. From reports of missing victims through fake reports of graffiti on the walls of a UK mosque, to warnings of armed men in certain neighbourhoods, false Tweets and Facebook posts undermined UK citizens' feelings of safety and trust in the media they received, exacerbating the impact of the bombings.

A recent BBC poll showed that 79% of respondents worry about fake news online. This speaks to a broader issue about trust in the sources of information that keep a democracy alive. As Adam Curtis pointed out in his recent

	documentary “Hypernormalisation”, if the public no longer believes any source of information, then the institutions of democracy and the West are undermined. Fake news is now one of the most powerful tools deployed against democracy.
How Singapore can combat online falsehoods	What are the solutions? Foreign governments offer not only problems, but also solutions to the issue of fake news, with both Germany and Canada leading the way. Disinformation campaigns in the American election prompted a measured vigilance against fake news on the part of the German government. All of the major parties publicly stated they would not use bots in their 2017 general election campaigns. Three German states have proposed digital trespassing initiatives, imposing fines on users who break platforms’ terms and conditions, criminalising the use of social bots on networked platforms like Facebook. A law was proposed to impose heavy fines on social platforms that failed to take down fake news, although this has raised a public and commercial outcry, with concerns around access to information and freedom of expression. The governing party proposed an end to anonymity on the internet, although this, too, has been shown to be unworkable as it violates German law. The issue is complex, particularly when operating within a civil society-driven legal framework, and attempting to balance a compulsion to regulate with the requirements of open democracy. Critical thinking skills around digital

and social media are vital to solving many of the issues of the connected society, including fake news.

Similarly, most German experts have recommended media literacy programmes as the most effective measure against fake news — it is our primary recommendation for action, running the gamut from early education programmes through adult media literacy.

The positive use of “transparency bots” is also an effective tool. In Canada, bots are used as automated agents drawing attention to prominent political actors and government agencies, highlighting, for example, the editing of a Wikipedia article by government agencies and political parties. Bots are also actively used by journalists to gather data. Political parties are using bots to disseminate information on vital legislation to voters. (And bots like Arachnid, soon to be used by the UK government, are being used to hunt down child pornography online.)

We also recommend the funding of an affordable software tool accessible to community leaders, allowing them to easily measure the impact of their civil society narrative initiatives on communities. This can be done through permission-based natural language processing and sentiment analysis algorithms, deployed in an environment encouraging trust.

Further, we believe the government should make significant increases in budgets for capacity development for civil society organisations engaged in counter-narrative programmes in the context of countering extremism. These include charity and open-journalism programmes, countering extremism programmes, and access-to-information programmes.

	These projects — both transparency bots and education initiatives — strengthen real news, edifying the institutions of democracy and the civil society. Undermining democracy and public faith in institutions is an essential tenet of hybrid warfare, whether practiced by foreign agents or home-grown extremists seeking to radicalise vulnerable citizens.
Principle that should guide Singapore's response	Constant vigilance, long-view approaches, and ongoing programmes of media education and literacy are vital to maintaining the interests and ideals of civil society and democracy. A version of this evidence was previously submitted by Dr Kriel to the UK's Digital, Culture, Media and Sports Select Committee, investigating Fake News.