FAKE NEWS: NATIONAL SECURITY IN THE POST-TRUTH ERA

Norman Vasu, Benjamin Ang, Terri-Anne-Teo, Shashi Jayakumar, Muhammad Faizal, and Juhi Ahuja
January 2018
Executive Summary

Fake news is not a new issue, but it poses a greater challenge now. The velocity of information has increased drastically with messages now spreading internationally within seconds online. Readers are overwhelmed by the flood of information, but older markers of veracity have not kept up, nor has there been a commensurate growth in the ability to counter false or fake news. These developments have given an opportunity to those seeking to destabilise a state or to push their perspectives to the fore. This report discusses fake news concerning the ways that it may manifest, how its dissemination is enabled through social media and search engines, how people are cognitively predisposed to imbibing it, and what are the various responses internationally that have been implemented or are being considered to counter it. This report finds that efforts to combat fake news must comprise both legislative and non-legislative approaches as each has its own challenges. First, the approaches must factor in an understanding of how technology enables fake news to spread and how people are predisposed to believe it. Second, it would be helpful to make a distinction between the different categories of falsehoods that are being propagated using social media. Third, efforts should go hand in hand with ongoing programmes at shoring up social resilience and national consensus. Fourth, efforts need to move beyond bland rebuttal and statements, as these may be counter-productive. Fifth, counter-narratives that challenge fake news must be released expeditiously as fake news can spread en masse at great speed due to technology. In sum, collaboration across the whole of society, including good public-private partnership, is necessary in order to expose fake news and ensure better synergy of efforts in countering it.
Introduction

Fake news is not new – consider for example the role played by the rumour of tallow and lard-greased cartridges in the Sepoy Mutiny of 1857 in India. Notwithstanding this, the issue poses a more significant challenge now. The velocity of information has increased drastically with messages now spreading internationally within seconds online. With countless photographs, opinions, and hours of footage published online, every falsehood can proliferate rapidly. Readers are overwhelmed by the flood of information, but older markers of veracity (respected publications, official sources) have not kept up, nor has there been a commensurate growth in the ability to counter false or fake news. In many cases, new, visually attractive, and sometimes false, sources of information are eclipsing publications of records such as newspapers. All this has given an opportunity to those seeking to destabilise a state or to push their perspectives to the fore. Modern disinformation operations only need free Twitter or Facebook accounts or access to platforms such as WhatsApp or Telegram.

This report is divided into five parts. The first section offers a survey of the various ways in which fake news may manifest. This unpacking of its various forms is essential for policy-making, as not all forms of fake news require the same attention of the state with regard to national security. The second section discusses how the dissemination of fake news is enabled by the manner in which social media platforms and search engines are programmed to offer curated information to what they consider are our interests. In addition, this section shows how such platforms and search engines have been exploited in order to distribute false information. The third section explains how we are cognitively predisposed to imbibing fake news. If we are to tackle this issue, this section offers the lay of the land of what we are cognitively up against. The penultimate section offers a survey and assessment of various responses internationally that have been put in place or are being considered to tackle fake news. The report concludes with several considerations that should be taken into account when developing approaches to counter the problem.
Unpacking Fake News

This section discusses how fake news may be understood as a range of phenomena. While there are many ways to categorise fake news, fake news is understood here as a medium for a spectrum of phenomena comprising five categories:

(i) Disinformation – falsehoods and rumours knowingly distributed to undermine national security, which can be part of state-sponsored disinformation campaigns;
(ii) Misinformation – falsehoods and rumours propagated as part of a political agenda by a domestic group/the relativisation/differing interpretation of facts based on ideological bias;
(iii) Misinformation – falsehoods and rumours propagated without a broad political aim, either with or without malicious intent that achieves viral status;
(iv) Entertainment – falsehoods used in parody, satire, or seemingly humorous pieces; and
(v) Falsehoods distributed for financial gain.

Disinformation Campaign to Undermine National Security

The first category, which this report is primarily concerned with, refers to the use of fake news as a medium for organised disinformation campaigns with the aim of destabilising states through the subversion of societies (and democratic processes including elections). This category is most onerous given its impact on national security and social cohesion.

In recent times, for example, these campaigns were reportedly carried out by Russia – using technological platforms – as part of broader influence operations in areas ranging from the Baltics to Central Europe to France to the United States. The magnitude of the Russian campaign to divide the American society was scrutinised in October/November 2017 during a

---

hearing where technological companies (Facebook, Twitter and Google) were questioned by the Senate Intelligence Committee. More details are discussed in the third section of this report.

**Misinformation for Domestic Political Agenda**

The second category covers a broad range. These include viral rumours or false information (or semi-truths) either shaping national opinion or affecting the resilience of a polity by actors within a state, without an external malign actor involved. This was evident in the 2016 presidential campaign in the United States (particularly on the part of the Trump campaign).

Separately, another example of this form of falsehood may be found in the lead up to the Brexit referendum in the United Kingdom. The “Leave” campaign resorted to tactics ranging from warnings about a country overrun by refugees and asylum seekers, to exaggerated claims that a sum of £350 million a week was being sent to Brussels by the UK government – money according to the claim would be saved if the Leave vote won.3

Finally, this form of falsehood has been seen in the growth of disinformation sources linked to groups from the alternative right (alt-right), with a denominator being anti-globalism and a strong distrust of the western, democratic sociopolitical model and neo-liberalism.

This second category of fake news may on certain occasions overlap with the first category. There is some suggestion, for example, that the Leave campaign in the UK may have received an impetus from Russian disinformation efforts in the lead up to the Brexit vote.4

---


Non-political Misinformation Gone Viral

The third category concerns viral falsehoods of an entirely different nature – for example, those achieving widespread currency in the wake of a disaster or terror attack. This is the third onerous category given its impact on public order and safety.

In the immediate aftermath of the 22 May 2017 Manchester terrorist attack, there was a significant circulation of fake news carried out by various groups and individuals. These ranged from the malicious (trolls) to the ignorant and misinformed. There were hoaxes of missing children (images of children pulled from the web) and also several other false stories, including claims of a man with a gun outside the Royal Oldham Hospital, situated near the scene of the attack.5

Separately, the immediate aftermath of the 13 April 2013 Boston Marathon bombing saw an outbreak of viral vigilantism. Individuals (many of them well-meaning), based on available images, attempted to crowdfund information and establish an identity on online bulletin boards. These individuals, abetted by journalists chasing what seemed like a plausible story, falsely identified a student who had been missing from Brown University for a month. This student was later found dead in a completely unrelated suicide, but the viral online vigilantism (entirely without repercussions to those who had made the accusations, or to the platform that had hosted many of the accusations, Reddit) placed immense strain on the grieving family.6


Another example of vigilantism with real world consequences (this time with a political motivation) concerns the case of Edgar Welch, who in December 2016 went to Comet Ping Pong Pizza Restaurant in Washington DC and fired shots from his automatic rifle after imbibing too deeply of the so-called “Pizzagate” conspiracy theory. The theory was dreamed up by internet trolls and fringe rightwing media, asserting, on the basis of some of John Podesta’s leaked e-mails, that the restaurant was the hub of an elite paedophile ring.
Falsehoods for Entertainment

The fourth category is the creation of fake stories for entertainment. Examples would include the offerings in the UK’s Punch magazine and online site *The Onion*. A by-product of this form of fake news is that some people may take the parody to be true. For example, China’s People’s Daily republished an *Onion* article claiming North Korea’s Kim Jong Un was voted 2012’s sexiest man alive.

This category might seem on the surface to be devoid of national security implications. Notable, however, is how seemingly humorous or satirical information can sometimes serve a nefarious purpose. Recent research has shown, for example, that there is an emerging form of fake news with a political purpose disguised as irony or satire/parody. People might try using irony to mainstream their extremist ideas or creeds by masquerading them as something else altogether.

A recent example from the United States is the so-called alt-right advancing its position using humorous and ironical facades. For this far-right movement, “irony has a strategic function. It allows people to disclaim a real commitment to far-right ideas while still espousing them … it also allows individuals to push boundaries in public, and to back away when they meet resistance.” A compounding difficulty for opponents of the “alt-right” is that it is not always simple to differentiate between sincerity and satirical online.

Falsehoods for Financial Gain

The fifth category concerns fake stories distributed in order to attain revenue from advertising or swaying sentiments to manipulate the stock market. This category is perhaps the least onerous given its non-security/non-political motivation but is nonetheless important due to its potential impact on social cohesion.

---


8 ibid.
Profit is the key motivator behind the creation of “news” in this category. Examples would be the Macedonian fake news “boiler houses” that invented fake stories on the US presidential elections.

If left unchecked, these may have a deleterious effect on society. The creators behind The Real Singapore (TRS), a socio-political Singapore website, began creating anti-foreigner comments on their website in 2012. These were found to have netted them over half a million Singapore dollars over a three-year period in online advertising. In the words of the public prosecutor, they were “wildly successful in their efforts to profit from the ill-will and hostility that they were peddling.” TRS’ founders were found guilty of sedition and deliberately sowing discord between Singaporeans and foreigners.9

Dissemination Techniques in Disinformation Campaigns

This section discusses the techniques used to disseminate fake news in disinformation campaigns (influence operations), particularly through the exploitation of social media platforms and search engines. The focus on disinformation campaigns stems from its detriment to national security and the possibility it could overlap with other (less onerous) categories of the fake news phenomena.

Russia

Many reports have discussed recent Russian influence operations attempting to manipulate democratic processes such as elections. These attempts were most conspicuous in the US 2016 presidential campaign. A declassified US intelligence assessment maintained that Russia used professional trolls and Russian state broadcaster Russia Today (RT) “as part of its influence efforts”. Succumbing to pressure from the US Department of Justice (DOJ), RT in November 2017 registered itself as an agent of a foreign government as

---

required by the US Foreign Agents Registration Act (FARA).\textsuperscript{10}

Russia reportedly paid thousands of people to create and peddle fake anti-Hillary Clinton news targeting key swing states. Russian hackers are also believed to be responsible for leaking e-mails from Democratic Party officials. Some credible experts have suggested that President Donald Trump and his team promoted narratives, including false ones, serving Russian interests.\textsuperscript{11}

It is worth considering how these influence operations took advantage of the most common ways for ordinary people to navigate the crowded information space: (i) search engines to look up information; and (ii) social media to find out what their social circles are saying, and/or to share their views with their circles. These systems have been developed over time, also in response to the flood of information, to create filter bubbles.

Google arranges and displays its search results based on an individual’s preferences which Google determines based on e-mail conversations, previous searches, viewing preferences on YouTube, and other personal data gathered through other Google applications. When Facebook displays posts on News Feeds, it only shows posts consistent with the user’s previous behaviour such as “liking” or sharing” other posts.

As a result, search results and social media feeds only show us results that cohere with what we already enjoy or believe hence creating filter bubbles or echo chambers. Fake news appearing to match or support these preferences or beliefs spreads quickly and is believable in this environment. One expert, the chief of Oxford Information Labs, holds that Facebook has an “insidious” effect on democratic societies, and also spoke of a “deeper, scarier, more insidious problem: we now exist in these curated environments, where we never see anything outside our own bubble … and we don’t realise how curated they are.”\textsuperscript{12}

\begin{itemize}
\end{itemize}
The creation of filter bubbles and echo chambers through the algorithms of search engines, and social media is further exploited by companies developing a model to translate social media data into a personality profile used to predict, and then influence user behaviour. For example, by correlating subjects’ Facebook Likes, building profiles, and data harvesting, Cambridge Analytica (CA) apparently can identify an individual’s gender, sexuality, political beliefs, and personality traits. This method also uses artificial intelligence (AI) to find out more about the individual, and is able to make accurate predictions on how to convince the individual to take certain actions with the appropriate sort of advert, while also creating a viral effect as there could also be other people in the individual’s network who subsequently like the same advert. CA was used by the Trump Campaign. During the 2016 US Presidential Election campaign, it was believed that Facebook users in key constituencies were targeted with personalised messages or fake news that played on their existing biases. This was just one aspect of the Trump data analytics campaign.13

Recent reports have suggested the FBI has collected data on (and is investigating) computer bots – programmes performing repetitive functions such as searches – allegedly linked to Russia and helped push negative information on Hillary Clinton and positive information on Donald Trump through Facebook and other social media platforms. This happened particularly in key battleground states, and the Russian disinformation apparatus was able to piggyback on it.14

Bots have also appeared elsewhere. Shortly before the French Presidential election, Facebook disabled 30,000 fake accounts in France – deleting them in some, but not all. Facebook (without assigning responsibility for these accounts) said its objective behind these takedowns is to remove fake accounts with high volumes of posting activity and the most prominent


audiences. It appears, however, the bots will be a feature of the social media landscape in the medium-term. Innovations in parallel computation and improvements to algorithm construction will make it harder to distinguish bots from humans. Some researchers believe that they have found fake Facebook groups almost entirely populated by bots. These fake groups, convincingly operated and orchestrated, eventually attracted real fans. It is possible that many Trump fans were emboldened to declare their support for the candidate due to the artificially created perception of a swell in support for him. Moreover, in this way, some of these originally-fake pages or groups swelled with real people, with the “fake” aspects of these groups withering away.

China

While far less has emerged from Chinese influence operations, the Chinese state apparatus reportedly has its version of “information troops” at its disposal. The great majority of these troops – called by some as the “50-cent army” – may not actually be part of the security apparatus, but independent operators including student volunteers at universities, Communist Youth League members, and government bureaucrats. They are also thought to be involved in faking several hundred million social media accounts. An example of the Chinese volunteer information

apparatus in action can be seen through the postings of Communist Youth League members in January 2017 when Tsai Ing-wen became the first female president elected in Taiwan. One analysis suggests a campaign started on a forum on Baidu to flood Tsai with anti-Taiwan comments. Within 12 hours, there were 40,000 negative comments on Tsai’s Facebook page, not done by any organised force, but by “volunteer armies of mobilised angry youth”.19

China is also believed to use non-technological methods for influence operations.20 There are some suggestions that in certain locations, China has attempted to infiltrate or influence organisations and individuals with the aim of pushing specific lines that fit with Beijing’s foreign policy or security objectives.21 For example, some analysts have suggested independence activists in Okinawa (regarded by most commentators as a fringe group) are backed by Chinese universities and think tanks. These efforts have not simply relied on informal efforts of the “50-cent army”.22

In another example, amid growing concerns of China’s influence operations in Australia, the Abbott government in early 2015 initiated a multi-agency effort to assess the magnitude of these operations.23 Among the conclusions from the assessment are that propaganda (e.g., pro-China publications) to shape the views of the general Australian public can be distributed through: (i) political donations to Australian politicians hence posing security risks to Australian policymaking; (ii) Chinese state-owned-enterprises and privately-
owned Chinese companies and associations; and (iii) engagements with non-Chinese businesses that rely on the Chinese market.24

Human Fallibility and Cognitive Predispositions

This section discusses how we are cognitively predisposed to imbibing fake news in general, and what we are cognitively up against. It is important to understand the issues of human fallibility and cognitive dispositions in order to develop approaches to counter fake news.25

Fallible Memory

The human memory is a fallible system, prone to error and distraction. The brain remembers information regardless of whether it is true or false. In this era of fake news and misinformation, individuals have a much more difficult time judging what is correct and incorrect. Human fallibility is also exacerbated by the technological landscape, with a growing body of scholarly work suggesting that the internet is changing the way we think, and making us more susceptible to irrelevance, rumour, and supposition. A 2009 meta-study by a development psychologist from the University of California, Los Angeles (UCLA) concluded that while the growing use of the internet had led to “new strengths in visual-spatial intelligence”, there had been a commensurate weakening of “deep processing” that underpinned “mindful knowledge acquisition, inductive analysis, critical thinking, imagination, and reflection.”26

Looking, searching and parsing information online have led to forms of shallowness. One study in 2009 saw Stanford researchers administering a battery of cognitive tests to two groups: heavy multitaskers and relatively light multitaskers. The former group was found to be much more easily

distracted by “irrelevant environmental stimuli” and had less ability to maintain concentration on a particular task, with some suggestion that those in this group may also have been “sacrificing performance on the primary task to let in other sources of information.”

Researchers also found that “skimming activity” was exhibited by individuals who use online resources. A study, done by researchers from University College London (UCL) that concluded in 2008, examined computer logs documenting user behaviour on two popular research databases. Individuals who used these databases quickly jumped from one source to another, only rarely returning to read in more depth a piece skimmed earlier.

If these behaviours are also found to be present in the general population that is receiving a significant proportion of their news from social media, it could indicate that they are not applying critical thinking to what they read, leaving them highly vulnerable to believing fake news.

Illusory Truth Effect

The illusory truth effect, as jointly examined by cognitive psychologists and neuroscientists, is the phenomena in which people, when exposed and then re-exposed to misinformation, would tend to believe that the information is more truthful because they cannot remember the original source of that information. Importantly, if people can remember that the original source of the misinformation is not credible, they can disqualify the information as being false. In the brain, these disqualification processes have been observed using neural signals found with both electroencephalography and functional magnetic resonance imaging.

---


Primacy Effect and Confirmation Bias

The primacy effect refers to the formative period where individuals form the most conclusive opinions as a result of information that is first acquired. Initial opinions tend to shape information in their favour despite being confronted by contesting and compelling evidence, which may not be accepted. This pattern of reinforcement is described as belief persistence, which involves “the mental representation and positive assessment of meaningful information”. Such behaviour is compounded by confirmation bias, which refers to the way in which individuals selectively seek or interpret evidence aligned with existing beliefs, values and hypotheses. This behaviour is conducted in an unwitting manner, which is a key characteristic of the bias.31

Access to Information

Individuals who are more exposed to fake news conveying messages about politics and politicians in comparison to hard news show a higher tendency to believe the former as the reality. This effect was investigated by researchers in a study on the 2006 Israeli general election campaign. The individuals' beliefs are maintained until hard news is conveyed to participants. The findings show that fake news only affects political attitudes if individuals believe that information conveyed within fake news accurately represents the political arena.32

Due to other environmental factors that affect voting behaviour, the study cannot conclusively show that there is a direct relationship between the consumption of fake news and election outcomes.

However, the findings of this study are significant for political communications where they show how fake news viewership could affect political attitudes, enhancing negative attitudes of inefficacy, alienation and cynicism towards politicians regardless of party affiliations. Comparatively, individuals who have a higher level of hard news consumption are better

---

attuned to recognise that it would be impossible for all politicians to be politically inept and morally questionable as much as the fake news suggests.

Individuals who already have set ideological predispositions are also more likely to believe in fake news. This effect was investigated by researchers in a study that found that ideologically aligned articles are more likely to be believed by heavy media consumers and those with segregated social networks because they are less likely to receive contradictory or opposing information from their peers. However, this study similarly could not make a conclusive correlation between fake news consumption and voting behaviour or voting patterns.33

Overall, there is still insufficient research that examines the relationship between the growing quantities of information available and how it is cognitively processed by individuals.

First, while past studies investigated the relationship between fake news consumption, set ideological predispositions and the likelihood to believe the information conveyed, it does not consider the cognitive abilities of media consumers, level of obligation to participate in elections and predispositions of cynicism.34

Second, the experience of information gathering may vary across generations. While the main unit of analysis in these studies is age, they show that knowledge of and access to technology correlates to the ability to access and critically analyse information online, and are, as such more reflective of the differences between digital natives and non-digital natives, rather than generational differences as defined by age. For example, a study shows how youths’ predilection for variety, fulfilled through online media, reflects an aversion to mainstream news such as televised networks or newspapers. Youths explain that the latter tend to be irrelevant to their needs and interests, or one-dimensional, and therefore lacking in credibility. A preference for news to be accessed instantly is also different from the

previous generations which are used to accessing news at a fixed time of day.\textsuperscript{35}

**International Responses to Fake News**

This section assesses the various approaches that have been implemented or are being considered to counter fake news internationally. Countries have different approaches based on the nature of fake news that affected them, and their respective domestic and geopolitical considerations.

**Counter Fake News Mechanisms**

Websites have been set up – by independent groups or states – as mechanisms to debunk fake news that constitute disinformation and other falsehoods. There are several examples from across the globe.

In Europe, Stopfake.org is a crowdsourced journalism project that was launched in 2014 to combat fake news spreading across the internet during Ukraine’s crisis in Crimea. The site checks facts, verifies information, and refutes inaccurate reports and propaganda about events in Crimea, which are widely believed to originate from Russia. Separately, there are existing fact-checking sites such as (i) http://www.snopes.com/, (ii) http://fakenewswatch.com/, (iii) http://realorsatire.com/, and (iv) https://mediabiasfactcheck.com/.

In Qatar, “Lift the Blockade” is a government website set up in September 2017 to counter what Qatar regards as fake news distributed by geopolitical rivals to justify the imposition of economic sanctions amid the gulf crisis.\textsuperscript{36}

In Singapore, “Factually” is a government website set up in 2012 to “clarify widespread misperceptions of government policy or incorrect assertions on


matters of public concern that can harm Singapore’s social fabric”.  

While important, these sites would not reach out to those who are not predisposed to fact-checking owing to their cognitive biases or due to digital illiteracy. Moreover, this form of debunking is slow. It requires an individual who is curious to uncover whether a news item is false by firstly, not sharing the item further; and secondly, fact checking at one of these sites. It also assumes that the reader will trust the findings of the fact checkers, whereas the fact checkers themselves are often accused of being biased; for example, Snopes has been labelled as “liberal”. Given the challenges, such websites should be run in tandem with wider strategic communications efforts.

**Strategic Communications**

Strategic communications efforts at the national (and regional) levels have been ramped up to counter fake news that constitutes disinformation. In Europe, the European Union’s External Action Service set up the East StratCom Task Force in September 2015, which runs the myth-busting website euvsdisinfo.eu. The task force also releases a weekly Disinformation Review – a review of the latest cases of news articles carrying key examples of how pro-Kremlin disinformation finds its way in international media, as well as news and analysis on the topic.  

The East StratCom Task Force operates on the existing EU strategic communication budget and is staffed by individuals from EU institutions or seconded from the EU Member States. It relies heavily on volunteers to both collect disinformation stories (more than 2,500 examples in 18 languages since 2015), and support the Disinformation Review.

Europe’s strategic communications efforts are also complemented by advocacy work done by think tanks. Their activities include: (i) publicly challenging supporters of Russian-sponsored disinformation; (ii) disclosing the disinformation campaign substance/vehicles; and (iii) systematically

---


building social resilience. This is important, as disinformation is most effective in states where citizens “exit” for political, economic, social, informational and cultural reasons; and where people are more vulnerable (to fake news) because they feel disenfranchised as the social contact between citizens and the state has weakened.

There can be merits in studying Europe’s strategic communications with the view of introducing similar efforts but tailored to other regions’ cultural and political landscape. These efforts also put pressure on social media companies to do more to counter fake news.

**Self-Regulation by Technological Companies**

The current spread of fake news, especially when it constitutes disinformation, is often attributed to social media platforms. Technological companies have long resisted being labelled as content publishers, but their ability to hold this line is weakening. Amid pressures from several governments, technological companies have instituted a mix of user-based and algorithmic-based initiatives since December 2016 for self-regulation.

One of the earlier measures is a tool enabling Facebook users to “flag” fake news reports for review by third-party fact-checkers from the International Fact Checking Network (IFCN). This initiative cooperates with media outlets in the EU Member States and became operational in March 2017. Similarly, China’s WeChat users can report other users and even entire chat groups for sharing false information, harassment, or gambling, by clicking a button on the profile page. The reports are examined by employees at WeChat who maintain a database of fake news used to sieve similar content to be blocked automatically if reposted in the future. WeChat has reportedly received 30,000 fake news reports and the system blocks about 2.1 million false rumour posts.\(^\text{39}\)

Ahead of the April 2017 French presidential elections, Facebook took a more proactive initiative of removing tens of thousands of fake accounts.

---

The fake accounts were identified by analysing patterns of activity (without necessarily assessing the content itself). In doing so, Facebook has employed algorithmic techniques, including machine learning, to target fake accounts – looking for “false amplifiers” of political stances, coordinated attempts to share and like certain posts, online harassment or the creation of “inflammatory or racist” content. These fake accounts would also include automated accounts (bots).40

Self-regulation initiatives that target content (and user accounts), however, have its limitations given that it has not sufficiently slowed down the spread of fake news.

Reducing Financial Incentives in Advertisements

Social media companies are exploring other methods. As seen from Facebook’s announcement, it will be hiring more than 1,000 people to review political advertisement purchases in order to better protect the US from the threat of disinformation through fake news.41

The method of targeting advertisement purchases essentially aims to reduce the volume of fake news by removing the financial incentive for its creation. This method can be employed against fake news used for disinformation campaigns and misinformation ( propagated without a broad political aim, either with or without malicious intent and achieving viral status).

This method, however, requires the private and public sectors to collaborate in exploring ways to alter the manner in which advertising revenue is generated online. It should be highlighted here that the private industry may not be averse to pulling out advertising from dubious sources.


websites as seen in cases of multinational companies that pulled their advertisements from alt-right websites in the US after being alerted.

Industry standards and codes of ethics can be established in order to institute more social accountability in online advertising by the private industry. This is one of the areas where legislation can give some teeth.

**Government Legislation**

Several governments are implementing or considering implementing new laws as a key measure to counter fake news. For such cases, the governments assessed that existing laws and regulations as well other approaches (counter fake news websites, strategic communications and self-regulation by social media companies) are inadequate.

Laws can hold technological companies accountable for the distribution of inaccurate information, and online advertisements that allow fake news to spread. For example, Germany, in October 2017, enacted a new law – The Network Enforcement Act – that could impose fines on social media companies if they continuously fail to remove illegal content including those that constitute hate speech and fake news. Israel is mooting the so-called “Facebook Bill” which would enable the state to issue injunctions to force social media companies to remove content that has been assessed by the police to be inciting hatred and violence; the first reading of the bill was passed in Knesset in March 2017.42 The US, in October 2017, announced the mooting of the bipartisan Senate bill – Honest Ads Act – that would give the state the power to compel companies to disclose information on buyers, and their expenditure and dissemination of online advertising that may be political43

Laws can also hold social media users accountable for the spread of fake news. For example, the Philippines, in August 2017, passed the Republic Act (RA) 10951, which gives the state the power (article 154) to penalise

---


individuals who “publish false news by passing it off as legitimate news through print or other publication methods” which “may endanger the public order, or cause damage to the interest or credit of the state”.44

Any state that seeks to criminalise the distribution of fake news or hold content providers responsible is bound to face certain challenges.

First, the criminalisation of the distribution of fake news will encounter a minefield of legal issues stemming from definitional problems while content providers, dependent upon where they are based, may attempt to evade national legislation. For example, Facebook has responded that the new German law requires social media platforms to delete content that is not clearly illegal, and this may be non-compliant with EU law.45

Second, there may be more political than technical constraints. For example, while German law is quite clear on what is hate speech, both the political left and right fear that the term “fake news” is open to exploitation, owing to its ambiguity. Moreover, there may be inherent biases when humans and machines (algorithms) endeavour to judge whether content is “manifestly” fake news. Hence, civil rights advocates and Facebook representatives are concerned that the law could have opposing effects on the freedom of expression.46

Third, while legislation seeks to hold technological companies and users accountable, it remains to be seen how legislation can add value in existing efforts to remove and deter automated accounts (bots). Currently, social media companies have introduced measures such as Facebook’s real-name policy and a ban on fake profiles, and Twitter’s bot policies to address the

Moreover, there is also the technical challenge of distinguishing malicious bots from those that spread legitimate information.\footnote{Meyer, David. “Can the Law Stop Fake News and Hoax-Spreading Bots? These Politicians Think So.” \textit{ZDnet}, January 24, 2017. www.zdnet.com/article/can-the-law-stop-fake-news-and-hoax-spreading-bots-these-politicians-think-so/}

Legislation against fake news is thus an emergent research space that requires further studies to assess its impact and possible amendments needed to ensure its efficacy in the long term. Given the challenges, legislation should be complemented with non-legislative measures; for example, this was indicated in the results of a public survey on fake news by the Singapore government in May 2017.\footnote{Chan, Luo Er. “New Laws on Fake News to be Introduced Next Year: Shanmugam.” \textit{Channel News Asia}, June 19, 2017. /www.channelnewsasia.com/news/singapore/new-laws-on-fake-news-to-be-introduced-next-year-shanmugam-8958048}

\section*{Critical Thinking and Media Literacy}

While legislation defines the unlawfulness in and addresses the distribution of fake news, a long-term solution would also require building social resilience so that opinions and emotions cannot be easily swayed by falsehoods. This is where the non-legislative measures – critical thinking and media literacy – have a role as a bulwark against falsehoods in general. For example, the Organisation for Economic Co-operation and Development’s (OECD) Director for Education has called for schools to teach children how to spot fake news and suggested that such skills be included in the criteria for PISA tests.\footnote{Coughlan, Sean. “Schools Should Teach Pupils How to Spot ‘Fake News’.” \textit{BBC}, March 18, 2017. www.bbc.com/news/education-39272841; and Bentzen, Naja. “Disinformation, ‘Fake News’ and the EU’s Response.” \textit{European Parliament Think Tank}, April 2, 2017. www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2017)608805}

Both critical thinking and media literacy entail teaching people to be more judicious in consuming information, including having the natural inclination to fact-check the materials they read. This encourages a culture shift: highlighting blind spots and biases, inciting a curiosity for information from a spectrum of sources, and training them to assess materials logically and consider alternative viewpoints, before reaching a conclusion. Given that
society today is highly digitised, technological tools such as apps (e.g., Open Mind) can be developed to facilitate critical thinking by aiding people in understanding their online surfing habits and associated biases.  

Instilling critical thinking skills in national education systems specifically with the aim of countering fake news is a new concept, with very few extant cases studies. However, there may be lessons from the CVE (Countering Violent Extremism) experience, where critical thinking skills, which are useful in steering youth away from radicalisation, can be applied to fake news. In addition, there are existing media literacy programmes such as the Safer Internet Day – promoting responsible use of digital technology – that is spearheaded in Singapore by the Media Literacy Council (MLC). Further studies should be done to determine how these programmes could be expanded to include fake news.

In the same vein as critical thinking, the CVE experience has shown that the source (or messenger) of counter-narratives matters. Official sources are important for trusted facts and information but may at times be counterproductive. For example, videos produced by the US Department of State (Centre for Strategic Counterterrorism Communications), to counter extremist messages have marginal credibility among certain target audiences. Hence, official sources including media and online platforms should be complemented by credible voices and face-to-face conversations. An example is the Our Singapore Conversation (OSC) initiative (2012-2013) which brought together individuals from diverse backgrounds and with different views to have dialogues on complex socioeconomic issues that are of concern to Singapore’s future.


Conclusion

There is no silver bullet. Efforts to counter fake news must comprise both legislative and non-legislative approaches – each has its own challenges – while taking into account several considerations.

First, these approaches must be grounded in an understanding of how technology enables fake news to spread, factoring in research on human predisposition to believing fake news (as well as the changing media consumption patterns of digital natives).

Second, it would help to make a distinction between the different categories of falsehoods that are being propagated using fake news as the medium. This includes grappling with the possibility of influence operations (disinformation) as those conducting it would seek to adapt their tactics in the long run in order to circumvent these approaches. Conflating all falsehoods as a homogeneous fake news phenomenon runs the risk of developing ineffective approaches.

Third, efforts to counter fake news should go hand in hand with ongoing programmes (e.g., critical thinking and media literacy) at shoring up social resilience and a national consensus. As UK political commentator and journalist, Matthew d’Ancona notes, post-truth is “what happens when a society relaxes its defence of the values that underpin its cohesion, order and progress: the values of veracity, honesty and accountability.” Framing the truth (or counter-messaging, as the case may be) is also important. Unpublished studies from Arizona State University (ASU), as an offshoot of work for the Defense Advanced Research Projects Agency (DARPA), may be of help with regard to developing persuasive counter-narratives. Studies done at ASU’s Department of Psychology and Department of Human Communication have highlighted how narratives have to have “fidelity” in order to be persuasive. Expressed simply, subjects will be more inclined to believe news if it corresponds to both their experiences

and, importantly, the stories they have heard before. Framing may be the key to persuasion.\(^{56}\)

Fourth, efforts need to move beyond bland rebuttals and statements. Research suggests that direct contradiction can be counter-productive and may instead cause individuals to become even more convinced of their beliefs.\(^{57}\) Since individuals respond best to persons and groups perceived to be more similar to them, collaborating with existing alternative news media outlets and social media companies like Facebook, which are seen as “authentic”, is an important step in gaining readership and credibility.\(^{58}\)

Fifth, counter-narratives that challenge fake news must be released expeditiously as fake news can spread *en masse* at great speed due to technology.\(^{59}\) Hence, efforts must be supported with good public-private partnerships (including with non-governmental entities and research institutes), given that technological companies such as Google and Facebook are working on developing tools (policies and artificial intelligence) to help identify potential fake news and to flag them accordingly.\(^{60}\) These tools can complement efforts by state agencies in using sentiment analysis and technology (data analytics and artificial intelligence) to identify potential flashpoints and develop counter-narratives.

Such partnerships require a collaborative rather than an adversarial relationship between states and technological companies. The relationship will become adversarial if states rely strictly on legislation to compel companies to counter fake news. This report has discussed the challenges with relying on legislation only. Moreover, the CVE experience has shown that purveyors of harmful content would seek to adapt their tactics to circumvent legislation such as by migrating to encrypted or closed

---

56 As D’Ancona notes, facts are not enough. They need to be “communicated in a way that recognises emotional as well as rational imperatives.”


58 Ibid, As D’Ancona notes, facts are not enough. They need to be “communicated in a way that recognises emotional as well as rational imperatives.”


60 Experts and social scientists were recruited during the Second World War by the US military machine in support of a psychological warfare campaign against the Nazi propaganda. American messaging was greatly enhanced by their input.
platforms (e.g., Telegram and WhatsApp) which are even harder to regulate.

In sum, fake news is a multidimensional problem, hence efforts to counter it must be multifaceted and grounded in a good understanding of the problem. Collaboration across the whole of society is necessary in order to unravel the problem and work towards a better synergy of efforts.
About the Authors

**Norman Vasu** is Senior Fellow and Deputy Head of the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Singapore. He received his MA from the University of Glasgow in 1998, an MSc in International Relations from the London School of Economics in 1999, and his PhD in International Politics from the University of Wales at Aberystwyth in 2004. He is the author of *How Diasporic Peoples Maintain their Identity in Multicultural Societies: Chinese, Africans, and Jews* (Edwin Mellen Press, 2008). Editor of *Social Resilience in Singapore: Reflections from the London Bombings* (Select Publishing, 2007), and co-editor of *Nations, National Narratives and Communities in the Asia Pacific* (Routledge, 2014) as well as *Immigration in Singapore* (Amsterdam University Press, 2015). His research on multiculturalism, ethnic relations, narratives of governance, citizenship, immigration and national security have been published in journals such as *Asian Survey*, *Asian Ethnicity*, *Journal of Comparative Asian Development* and *The Copenhagen Journal of Asian Studies* and a number of edited volumes. He was a Fulbright Fellow with the Center for Strategic Communication, Hugh Downs School of Human Communication, Arizona State University in 2012.

**Benjamin Ang** joined the Centre of Excellence for National Security (CENS) at RSIS as a Senior Fellow in cybersecurity issues in February 2016. Prior to this, he had a multi-faceted career that included time as a litigation lawyer arguing commercial cases, IT director and general manager of a major Singapore law firm, corporate lawyer specialising in technology law and intellectual property issues, in-house legal counsel in an international software company, Director-Asia in a regional technology consulting firm, in-house legal counsel in a transmedia company, and senior law lecturer at a local Polytechnic, specialising in data privacy, digital forensics, and computer misuse and cybersecurity. Benjamin graduated from Law School at the National University of Singapore, and has an MBA and Masters of Science in Management Information Systems (MS-MIS) from Boston University. He is qualified as an advocate and solicitor of the Supreme Court of Singapore. He is also a Certified Novell Network administrator.
Terri-Anne Teo is a Research Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. She holds a PhD in Politics from the University of Bristol. Before joining RSIS, Terri-Anne taught courses on Political Theory and World Politics at the University of Bristol, and guest lectured at Singapore Management University (SMU), on multiculturalism in Singapore. Her research focuses on the theory of multiculturalism, citizenship and postcolonialism.

Shashi Jayakumar assumed the appointment as Head, Centre of Excellence for National Security (CENS) on 1 April 2015, and the appointment of Executive Coordinator, Future Issues and Technology on 1 August 2017. Dr Jayakumar was educated at Oxford University where he studied History (BA 1997, D.Phil. 2001). He has published in various peer-reviewed journals and edited volumes on topics relating to medieval history (the focus of his doctorate). He was a member of the Singapore Administrative Service from 2002-2017. During this time, he was posted to various ministries, including the Ministries of Defence, Manpower, Information and the Arts, Community Development, and Youth and Sports. From August 2011-July 2014, he was a Senior Visiting Research Fellow at the Lee Kuan Yew School of Public Policy. His research interests include extremism, social resilience, cyber, and homeland defence. He is currently completing a book relating to local (Singapore) politics (forthcoming, National University of Singapore Press, 2018).

Muhammad Faizal is a Research Fellow with the Centre of Excellence for National Security (CENS), at the S. Rajaratnam School of International Studies (RSIS). He holds a Bachelor of Business Administration (with Merit), from the National University of Singapore. Prior to joining RSIS, Faizal served with the Singapore Ministry of Home Affairs where he was a deputy director and had facilitated international engagements with foreign security counterparts. He also had postings in the Singapore Police Force where he supervised and performed intelligence analysis, achieving several commendation awards including the Minister for Home Affairs National Day Award (2009), for operational and analysis efficiency; and in the National Security Research Centre (NSRC), at the National Security Coordination Secretariat (NSCS), where he led a team to research emergent trends in domestic security and monitor terrorism-related developments. Faizal also has certifications in Counter-Terrorism, Crime Prevention and Business Continuity Planning.
Juhi Ahuja is a Senior Analyst at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). Prior to joining CENS, Juhi was a Research Analyst with the Studies in Inter-Religious Relations in Plural Societies (SRP) Programme at RSIS. She holds an MSc in International Relations from RSIS, and was awarded the SRP Study Award. She previously worked at the Embassy of Timor-Leste in Singapore, as an Economic & Trade Officer. Her research interests include religious violence and extremism, socio-cultural identity, postcolonial theory, and nationalism.
About the Centre of Excellence for National Security

The Centre of Excellence for National Security (CENS) is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d’être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting-edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information about CENS, please visit https://www.rsis.edu.sg/research/cens/.

About the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS’ mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS’ activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg.