

## Additional information for the Joint Standing Committee on Electoral Matters:

---

*Inquiry into and report on all aspects of the conduct of the 2016 federal Election and matters related thereto*

Following N&MRC members' testimony on 20 November 2018, the chair requested additional information regarding:

1. Foreign influence operations; and
2. Policies and tools to address misinformation.

Please find attached those further contributions. Please do not hesitate to contact the N&MRC for any further information.

Kind regards,

Caroline Fisher

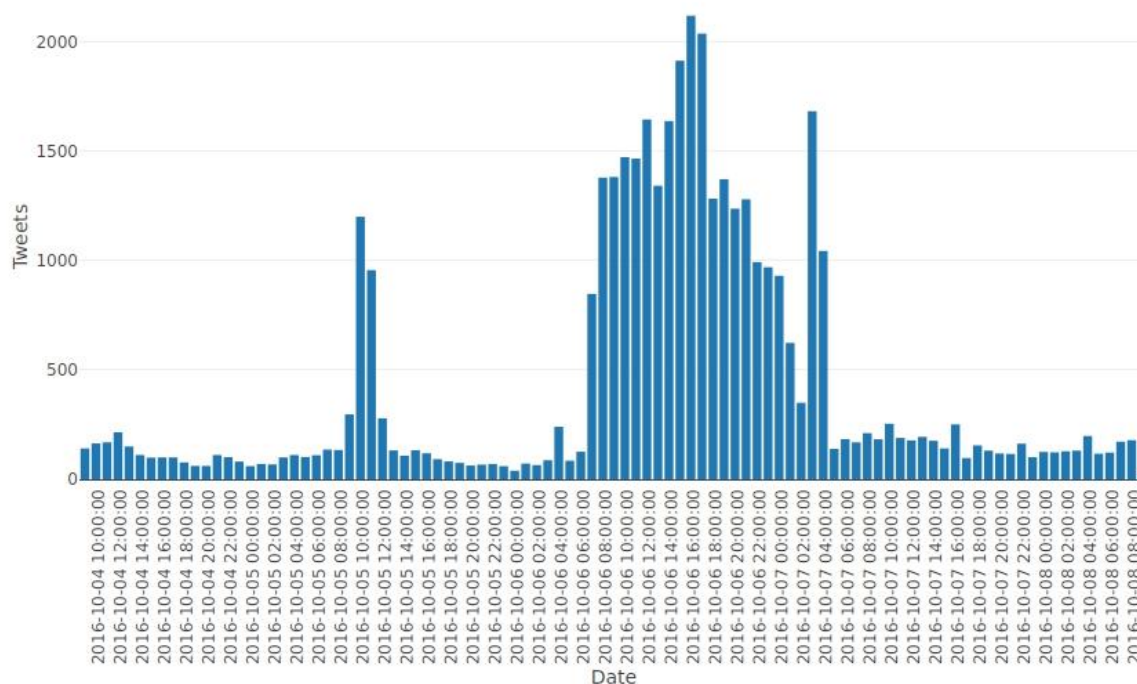
## PART 1. Foreign influence operations

### Additional evidence provided by Dr Mike Jensen:

In this section, Dr Jensen extends his testimony to emphasize the strategic significance of influence operations and discuss in greater detail the need for a whole-of-society response.

There are three points to make. Firstly, the concern posed by foreign influence operations goes beyond the narrow windows of political campaign periods. Particularly when there is little daylight between the major parties regarding the strategic interests of foreign powers they may seek to reshape societal attitudes. This requires a long-term investment in messaging through media platforms, digital spaces, foreign supported cultural organisations, think tanks, university research centres, and even working with domestic activist organisations.

Secondly, the data below provides a better sense of what Russia's influence operation looked like in 2016. Below is an hour-by-hour plot of tweets for the most active single day period of tweeting during the 2016 US election. This occurred on 6 October.



Note that the level of Russian engagement on Twitter picks up at 7 AM local time for the Eastern United States and continues until 5 AM the following day. These data suggest there was a specific objective they sought to achieve on that day.

The timing of this activity is consistent with the theory that the Internet Research Agency was acting on information likely obtainable only through Russian espionage. This was not the only time they engaged in a sustained period of operation targeting American politics during the campaign.

Finally, in addressing the issues posed by foreign influence operations, a multipronged response is necessary to secure the integrity of the public sphere. We can divide the relevant actors into domestic governmental actors, foreign governments and other organised interests (for example, the range of actors required to register under FITS), online platforms, and domestic civil society. I will briefly discuss each in turn.

### Government

The national security community has a critical role to play in identifying and attributing organised influence activities. Attribution is particularly important given the legal circumstances around the distinction between foreign and domestic actors.

### Foreign governments/organised interests

The Australian government can leverage its diplomatic, intelligence, national security, and economic capabilities to deter the execution of influence operations against Australia. These responses are likely to be most effective when used in concert, which would require strong interagency coordination in the execution of responses.

### Platforms

The role of platforms is a matter which requires further consideration regarding their responsibilities. This involves tricky normative issues which cannot be resolved here. However, it would seem reasonable that appropriate law enforcement agencies should be able to count on the cooperation of platforms in identifying and attributing organised foreign influence operations that run afoul of Australian law – and that platforms agree to suspend accounts associated with influence activities. This would mirror the level of cooperation detailed in recent public reports about the coordination between law enforcement and social media platforms before the 2018 US midterm elections.

### Civil society

Civil society actors can play important roles in both educating the public about news literacy and presenting public evidence of ongoing information operations. While intelligence agencies can track these operations, they are often limited in what they can make public in real time. This is an area where research centres and academics can play a critical role in educating the public – particularly to the extent that they can stand apart from the appearance of partisan interests. At the same time, where appropriate, these efforts can be aided by building relationships between law enforcement and the national security community with individual academics and research centres so that the efforts outside of government can be better directed.

As influence operations continue to evolve, we run the risk of preparing to defend against the last attack and fail to imagine what the future will bring. For this reason, strong communication ties between government agencies, platforms, and civil society are important to anticipating future threats to Australian democracy.

## PART 2. Misinformation

Additional information provided by Assoc. Prof. Mathieu O’Neil,

### Summary

Internet communication is posing two interlocked challenges to Australian democracy: hostile strategic actors are attempting to sow division in society by weaponising controversial or misleading information; the self-selection of news and disappearance of attitude-challenging content in some parts of the population’s news diet can lead to the rise of ‘echo chambers’ which facilitate the dissemination of misinformed opinion. A diverse range of entities such as States, social networking platforms, higher-learning institutions, non-profits and news media organisations have proposed solutions to counter misinformation. These notes provide a brief overview of some notable instances, briefly review the psychology of belief and debunking, and outline further proposals to counter the dissemination of misinformation.

### 1. Existing solutions

#### Education and media literacy initiatives

Several initiatives have created online verification tools and games intended to help people learn to recognize signals of source incredibility (such as hyper-partisan claims and emotionally charged headlines). Other initiatives aim to develop the public’s media literacy. A table of useful tools can be found in the Appendix of the N&MRC’s original submission, and is elaborated on here.

**First Draft**, led by digital expert Clair Wardle, is a project of the Shorenstein Center on Media, Politics and Public Policy at Harvard University’s John F. Kennedy School of Government. Its stated aim is to use research-based methods to fight mis- and disinformation online and provide practical and ethical guidance in how to find, verify and publish content sourced from the social web. You can find their work here: <https://firstdraftnews.org/>

A former journalist, Steve Brill, developed a news ranking system called **NewsGuard** which rates the quality of news sources using a traffic light coding. According to survey research (by <https://www.knightfoundation.org/reports/assessing-the-effect-of-news-source-ratings-on-news-content>) this red, orange and green ranking system was deemed very effective by users.

The Sage publishing company has launched a Fake news game, **Factitious**, where students can evaluate whether a news story is real or fake: <http://factitious.augamestudio.com/#/>

The Center for Complex Networks and Systems Research at Indiana has released **Fakey**, a mobile news literacy game which simulates a typical social media news feed, with a mix of news articles from mainstream and low-credibility sources. Players get more points for sharing news from reliable sources and flagging suspicious content for fact-checking. See <https://fakey.iuni.iu.edu/>

**Media Literacy Week** was an Australian Broadcasting Corporation initiative aimed at ‘equipping Australians of all ages with the skills they need to understand and interpret news and information’. During September 10-16, 2018, the ABC shared tips for navigating the modern media landscape, including methods to spot whether videos have been tampered with.

See <http://www.abc.net.au/news/story-streams/media-literacy-week/>

Finally **Melissa Zimdars** (Merrimack College) compiled in 2016 a well-regarded list of ‘False, Misleading, Clickbait-y, and/or Satirical “News” Sources’ which also featured a comprehensive selection of discursive, stylistic, behavioural, etc indicators that sites may be fake.

See [https://docs.google.com/document/d/10eA5-mCZLSS4MQY5QG5ewC3VAL6pLkT53V\\_81ZyitM/preview](https://docs.google.com/document/d/10eA5-mCZLSS4MQY5QG5ewC3VAL6pLkT53V_81ZyitM/preview)

## Journalistic practice & academic research

A range of **academic research** has been conducted to examine the extent of foreign interference and misinformation in elections. Two recent reports are mentioned here:

The Mass Communication Research Center at the University of Wisconsin-Madison published a comprehensive account of the Influence of the Russian Internet Research Agency (IRA), ‘The Twitter Exploit: How Russian Propaganda Infiltrated U.S. News’, demonstrating that the influence of IRA accounts extended beyond social media, into US News media. Searching 33 major media outlets during and after the 2016 election, the authors found 32 outlets with at least one story that embedded a tweet from IRA accounts (a total of 116 articles).

See <https://mcrc.journalism.wisc.edu/2018/05/08/the-twitter-exploit-how-russian-propaganda-infiltrated-u-s-news/>

Dr Jason Cabañes (University of Leeds) and Dr Jonathan Corpus Ong (University of Massachusetts Amherst) produced an account of the operation of troll farms in the Philippines, published in February 2018: ‘Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines’.

<https://media.leeds.ac.uk/news/architects-of-networked-disinformation-report-published/>

**Journalism** has been deployed against disinformation in traditional fashion (the uncovering of hidden truths). Magazines such as *Rolling Stone* and *Esquire* have conducted extensive investigative exposes of ‘trolling’ campaigns.

See for ex <https://www.esquire.com/news-politics/a51713/how-internet-trolls-won-in-2016/>

New methods have also been introduced, such as reporting on ‘what the other side is saying’ or ‘crowdsourcing’ audiences to help counter false information.

*The Guardian* proposes overviews of ‘alt-right’ media called ‘Burst Your Bubble’, described as a ‘weekly guide to conservative articles worth reading to expand your thinking’.

See <https://www.theguardian.com/us-news/series/burst-your-bubble>

US progressive magazine *Mother Jones* proposes to recruit audiences in a crowdsourcing effort to spot and denounce fake news by ‘signing up as a disinformation lookout’.

See <https://www.motherjones.com/media/2018/05/help-spot-disinformation/>

## Technological fixes

The homophilious nature of social networks (people connect primarily to people like themselves) may result in a lack of exposure to attitude-challenging information. The emotional appeal of sensational content means it is more likely to be shared and to spread quickly. These factors make users vulnerable to disinformation. Nonetheless some organisations believe that technology itself can provide automated solutions enabling news consumers to discriminate between fact and fiction.

French newspaper *Le Monde* launched its **Decodex** initiative in 2017. This comprises a site offering tips on how to evaluate information reliability, a Firefox or Chrome browser Plugin which is meant to indicate whether a site is trustworthy or not, and a virtual assistant for Facebook Messenger.

See <https://chrome.google.com/webstore/detail/decodex/kbpkclapffgmndlaifaaalgaagkfdod>

Also from the Center for Complex Networks and Systems Research comes **Hoaxy** (a system that tracks and visualizes the spread of content from low-credibility sources, and how it competes with fact-checking content) as well as **Botometer** (which checks the activity of a Twitter account and gives it a score based on how likely the account is to be an automated ‘bot’; higher scores are more bot-like).

See <http://hoaxy.iuni.iu.edu/> and <https://botometer.iuni.iu.edu/#!/>

Facebook has provided its own solution – algorithmically identifying misinformation and reducing its visibility in users’ feeds.

See <https://newsroom.fb.com/news/2018/01/trusted-sources/>

Facebook has also recently teamed up with the Atlantic Council’s Digital Forensic Research Lab (DFRLab) to provide ‘real-time insights and updates on emerging threats and disinformation campaigns’ during elections.

See <https://newsroom.fb.com/news/2018/05/announcing-new-election-partnership-with-the-atlantic-council/>

However, attempts by Facebook and other SNS and messaging platforms, such as WhatsApp, Twitter and YouTube, have attracted criticism because of their inability or unwillingness to address these issues in a systemic manner.

See for ex: <https://www.canberratimes.com.au/world/north-america/delay-deny-deflect-facebook-s-russian-propaganda-crisis-playbook-20181115-p50g6l.html>

## Legislative solutions

Several countries have attempted to implement legislative solutions to combat disinformation and foreign interference in elections. Legislation was passed in France in early July 2018, however a wide range of opposition parties (from the far-right to the far-left) raised objections, as the definition of ‘fake news’ was deemed too vague and there were concerns that freedom of expression might be imperilled.

See <https://www.theguardian.com/world/2018/jun/07/france-macron-fake-news-law-criticised-parliament>

The legislation does not target authors of misinformation but instead the digital platforms which disseminate them. This raises the issue of the transparency of the algorithms which channel news to users, and of the challenges when dealing with non-traditional media platforms such as Facebook.

The Poynter research organisation has compiled a useful guide to existing legislative approaches to misinformation around the world, which you can find here:

<https://www.poynter.org/news/guide-anti-misinformation-actions-around-world>

A draft white paper on legislative and other remedies (such as a duty on the part of platforms to identify inauthentic accounts) was released by US Senator Mark Warner and is also very useful in this regard. It can be found here:

[https://regmedia.co.uk/2018/07/30/warner\\_social\\_media\\_proposal.pdf](https://regmedia.co.uk/2018/07/30/warner_social_media_proposal.pdf)

## 2. The psychology of belief and effective debunking

Many of these existing solutions have benefits, but none of them address a central area of concern: how is it possible to overcome self-confirmation bias and the attendant rejection of cognitive dissonance, which make people who are wedded to a factually incorrect notion reluctant to relinquish it when confronted with a correct one?

Reaching people who are wedded to incorrect ideas without giving them the impression that they are being condescended to (or that the rebuttal is somehow part of a mendacious conspiracy) necessitates referring to some elementary principles of psychology, as outlined for example in Schwartz & Newman (2017):

When knowledge is uncertain, people turn to social consensus to gauge what is likely to be correct (Festinger, 1954) — if many people believe it, there's probably something to it. Hence, people are more confident in their beliefs if others share them (Visser & Mirabile, 2004) and more inclined to believe scientific theories when there is consensus among scientists (Lewandowsky, Gignac, Vaughan, 2013). But determining the extent of consensus can be difficult and familiarity offers a plausible shortcut — if many people think so, one should have heard it a few times, making it familiar. This gives small but vocal groups a great advantage — the more often they repeat their message, the more familiar it feels and the more people infer that many others agree, even if every repetition comes from the same source.

It is also relevant to refer briefly to climate scientists who have had to confront incorrect beliefs. Some scientists have identified key risks when confronting incorrect beliefs, as well as strategies to address them (see Cook & Lewandowski 2012):

### *The Familiarity Backfire Effect*

To debunk a myth, you often have to mention it - otherwise, how will people know what you're talking about? However, this makes people more familiar with the myth and hence more likely to accept it as true.



#### *The Overkill Backfire Effect*

Common wisdom is that the more counter-arguments you provide, the more successful you'll be in debunking a myth. It turns out that the opposite can be true. When it comes to refuting misinformation, less can be more.

#### *The Worldview Backfire Effect*

For those who are strongly fixed in their views, being confronted with counter-arguments can cause their views to be strengthened.

#### *Filling the gap with an alternative explanation*

For the alternative to be accepted, it must be plausible and explain all observed features of the event. When you debunk a myth, you create a gap in the person's mind. To be effective, your debunking must fill that gap.

### 3. Recommendations

In addition to the recommendations of the N&MRC's original submission, a proactive strategy for government to counter disinformation might include the following:

#### Media literacy education of the general public

It would be possible to condense Melissa Zimdar's abovementioned indicators that sites may be dishonest into (for ex.) 5 or 10 key points. These key points to identify false information could then be widely circulated. Jensen & O'Neil (2018) provided a précis which could also be used as a base, to wit: 'grammatical errors, mistakes regarding noncontroversial facts, lack of sourcing, factual claims being linked to a political agenda, and links to sources which do not back up the claims of the article, are often indications that a news story is dubious at best.'

#### Media literacy in schools

See recommendation in original N&MRC submission to Committee (p. 19) about inclusion of media literacy in school curricula. The existence of deepfakes ('artificial intelligence-based human image synthesis technique used to combine and superimpose existing images and videos onto source images or videos') means realistic fake videos can now be produced. The development of visual literacies to identify doctored images (as proposed by the ABC during its abovementioned Media Literacy Week for example) should also be encouraged. However as stated to the Committee, media literacy alone is not enough: knowledge of history is also paramount.

#### Information campaigns

As stated previously Internet communication is posing two interlocked challenges to democracies: hostile strategic actors are attempting to sow division in society by weaponising controversial or misleading information; the self-selection of news can result in the increasing disappearance of attitude-challenging content in some parts of the population, in turn leading to the spread of misinformed opinion. The Australian response to what Harvard expert Clair Wardle calls a generalised 'information disorder' (Wardle & Derakhshan 2017) ought to be multipronged and whole-of-government. Possible themes might include:



- Bringing people together: Emphasis should be placed on what unites the nation, on common values in a multicultural society;
- The value of open debate and historical knowledge: the strength of democracies is that they can confront and debate past and present social conflicts openly, leading to increased understanding and respect. Authoritarian regimes are unwilling to do so and this contrast could be made clearer.

More specific principles to combat misinformation might include:

- Identification of key areas which are likely to be targeted by hostile strategic actors to increase social divisions (for ex. zones of inter-racial or inter-religious tension or any other topic where strong, contrasting opinions are held);
- Anti-misinformation messaging should repeat key facts in ways that make them easy to be processed, i.e., the truth should be rendered as ‘fluent and familiar’ as possible;
- Because truth is often more complex than falsehoods, anti-misinformation messaging must strive for clarity, repetition, and avoid reiterating incorrect assertions;
- Anti-misinformation messaging should use credible third-party endorsements to rebut or support claims, not just political players. In addition, research shows that the spokesperson refuting the rumor should be an unlikely source, someone whose personal and political interests would be better served if the rumor were true (Berinsky, 2017) (e.g. misinformation that skews right will be better countered by right-wing politician than by a non-partisan organisation);
- Government could promote or legislate the use of a labelling scheme that clearly identifies ‘real’ versus ‘fake’ news.

## References

Berinsky (2017) ‘This is how you stop fake news’. *Washington Post*, 28 March.

Available at: [https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/28/this-is-how-you-stop-fake-news/?utm\\_term=.2ddcba72d773](https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/28/this-is-how-you-stop-fake-news/?utm_term=.2ddcba72d773)

Cook & Lewandowski (2012) ‘The Debunking Handbook’. UQ/UWA.

Available at: <https://www.skepticalscience.com/Debunking-Handbook-now-freely-available-download.html>

Jensen & O’Neil (2018) ‘Fake News, Real Problems: What is disinformation and how do we confront it?’ Park et al., Digital New Report, News & Media Research Centre, University of Canberra.

Available at: <http://apo.org.au/node/174861>

Schwartz & Newman (2017) ‘How does the gut know truth? The psychology of “truthiness”’. APA Science Brief.

Available at: <https://www.apa.org/science/about/psa/2017/08/gut-truth.aspx>

Wardle & Derakhshan (2017) 'Information Disorder: Toward an interdisciplinary framework for research and policymaking'. Council of Europe.

Available at: <https://shorensteincenter.org/information-disorder-framework-for-research-and-policy-making/>