Australian Government
Department of Home Affairs

Submission into the Senate Select Committee on Foreign Interference through Social Media

Table of Contents

1. The Department of Home Affairs (the Department) and its portfolio agencies welcome the opportunity to provide a submission to the Select Committee on Foreign Interference through Social Media. Foreign interference continues to present challenges to Australia's sovereignty, values and national interests at levels which the Director General of Security has described as unprecedented. Globally, some state actors persist in undertaking targeted activities designed to interfere in the operation and decision-making of other nations, shape political discourse, effect and undermine social norms and further their own interests.
2. Foreign interference occurs through a range of vectors. **People** can be corrupted, deceived or coerced into acting for, or on behalf of, a foreign actor. **Infrastructure** can be degraded, controlled or accessed to achieve a purpose for a foreign actor. I**nformation** can be stolen, manipulated or fabricated to achieve a purpose which is in the strategic interest of a foreign actor. Social media can be a particularly effective tool in the manipulation of information. Hostile foreign actors actively use social media to promote narratives and spread disinformation which serve their strategic interests, undermine democratic processes and institutions, and stifle dissenting voices.
3. The increasing use of social media as a source of information and for personal engagement on social and community issues, means that social media platforms can be used to disseminate and quickly amplify misinformation or promulgate political views in a manner which allows the principal author to remain anonymous. The combination of these activities alongside ill-informed or deliberately divisive commentary, broad and issue-specific political advocacy or financially motivated disinformation (i.e. 'clickbait') can complicate, or in some cases negate, attribution. The international nature of the most popular social media platforms and the importance of long-held democratic values of free and open expression make moderation or regulatory responses complicated.

Foreign Interference

4. Foreign interference activity against Australian interests is occurring at an unprecedented scale. In some instances the harm from foreign interference is immediately evident, while in other cases it might not materialise for years or potentially decades. The threat is insidious.
5. Foreign interference, if left unchecked, can exploit Australia's way of life and open system of government to erode our sovereignty. Acts of foreign interference can limit the Australian polity's ability to make independent judgements and can corrupt the integrity of Australia's systems. Such acts can also erode public confidence in our political and government institutions and can interfere with private sector decision-making to the detriment of our national security and economic prosperity.
6. Protecting Australia's sovereignty, values and national interests from foreign interference forms the core of Australia's response to foreign interference.

Definitions

- *Foreign Interference*: Clandestine activities carried out by, or on behalf of, a foreign actor which seek to interfere in decision-making, political discourse or other societal norms. Foreign interference is coercive, covert, deceptive or corrupting and is contrary to Australia's sovereignty, values and national interests.
- *Foreign Influence*: Overt activities to advocate for particular outcomes or shape consideration of issues important to foreign actors. When conducted in an open and transparent manner, these activities can contribute positively to public debate.
- *Disinformation*: False information designed to deliberately mislead and influence public opinion or obscure the truth for malicious or deceptive purposes. Disinformation can be intended for financial gain (such as clickbait stories), but have an incidental effect on public opinion or debate.[i]
- *Misinformation*: False information that is spread due to ignorance, by error or mistake with good intentions/without the intent to deceive.[ii]

[i] Adapted from academic literature about disinformation and the United Kingdom Home Office's Research, Information and Communications Unit's definition of disinformation that includes the key words 'deliberate' and 'malicious'.

[ii] Jennifer Kavanagh, Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life, 2018, RAND Corporation, p.10.

The use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation

7. Social media enables people across the world to engage in public debate about issues, public policy, ideologies and politics. It serves as a source of commentary operating at least in parallel to, if not in large part supplanting, traditional media. Generally, users can selectively follow and engage with individuals, groups, businesses and political parties of interest to them. Therefore, social media platforms can provide a relatively low cost and easily accessible tool with which to engage large populations.
8. In addition, social media can selectively deliver tailored messaging through the micro-targeting of audiences identified by 'big data' analytics. This is generally the result of previous behaviours displayed by the user, or based upon the network of people or groups they follow. The delivery of different messages to different audiences is very much a feature of the 'echo chamber' effect which can drive political and social polarisation on social media. This can occur when users are continually receiving self-reinforcing communications based upon their previous online behaviours or social networks, at the expense of different views or information.
9. Social media is an ideal platform for propaganda. The platforms are largely globalised and in many cases fall outside the regulatory arrangements for traditional media, broadcasting, and communications and carriage service providers. Additionally, the platforms are accessed by billions of people and are intrusive of privacy in ways that support tailored messaging. In the worst cases, the platforms can be used to promulgate 'fake news' and provocatively partisan content, undermine social cohesion and sow discontent (or at least confusion).
    - Hateful, inauthentic, and divisive disinformation can undermine social cohesion. Disinformation could be used to interfere with Australia's way of life or drive division within our society. This could be particularly potent at times of heightened community stress or anxiety, including if deployed tactically during a natural disaster or in the immediate aftermath of a terrorism incident.

10. Foreign state actors can promulgate propaganda and disinformation through social media in their attempts to influence communities and broader public opinion on matters of importance to them – though attribution is often difficult. The open and apparently democratic nature of social media, where all users are free to express their own views (subject to terms of use) on political and social issues, irrespective of their expertise or credentials, provides an ideal environment through which to seed disinformation.

11. Social media may also be used by foreign state actors to sow distrust and division in the Australian community or to shape community perceptions about the governing regime of the foreign state in a manner in which their involvement is not readily apparent. This could extend to promoting views contrary to Australian Government positions where those conflict with their interests, or otherwise seeking to control the online narrative and discussion of 'sensitive topics'. This could undermine social cohesion and Australia's free and open society if it is targeted towards culturally and linguistically diverse groups.

    - While major social media companies such as Facebook and Twitter, due to their size and reach, are currently the main conduits of digital disinformation in Australia, other smaller companies and platforms have been misused as well. For example, in 2018 Business Insider Australia compiled a list of 16 platforms, sites, and digital service providers that had been used for the dissemination of disinformation; including the mobile game Pokemon Go, group-hosting site Meet Up, and social media network Gab.[1]

12. Noting recent events overseas, the manipulation by foreign states of social media during Australia's electoral processes is a realistic prospect for federal, state and territory elections. However, foreign state-sponsored social media campaigns can be conducted at any time in response to geopolitical developments and not just during elections.

13. The growing presence and use of social media platforms in Australia that are extensions of social platforms in authoritarian states may require additional responses, as censorship and reduced privacy protections become additional concerns.

Vulnerability to interference through social media

- In 2019, Oxford University estimated that 70 countries around the world were involved in organised social media manipulation campaigns, up from 48 in 2018 and 28 in 2017.[iii] Stanford University has identified 570 deceptive 'news' websites receiving over 70 million monthly engagements on Facebook—a volume comparable to mainstream media outlets.[iv] MIT has concluded that false news stories are 70 percent more likely to be shared on Twitter than true stories, and that they reach 1,500 people in a sixth of the time.[v]
- Interference and manipulation of information through social media is a global and growing trend, and Australia is not immune. A 2019 University of Canberra study found social media is now the primary source of news for 47 percent of people born in the 1990s and 33 percent of people born in the 1980s.[vi]

[iii] *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, University of Oxford, UK, 2019.

[iv] Hunt Allcott, et al., "Trends in the diffusion of misinformation on social media", *Research and Politics,* Vol. 1., No. 8, April-June 2019.

[v] "Study: on Twitter, false news travels faster than true stories", MIT News, 8 March 2019, online at: http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

[vi] https://apo.org.au/sites/default/files/resource-files/2019/06/apo-nid240786-1366986.pdf.

[1] "Russia's disinformation campaign wasn't just on Facebook and Twitter. Here are all the social media platforms Russian trolls weaponised during the 2016 US elections", Business Insider Australia, 19 December 2018, online at: https://www.businessinsider.com.au/all-social-apps-russian-trolls-used-spread-disinformation-2018-12

Algorithms and online 'echo-chambers'

- The algorithms that drive social media platforms can be exploited by hostile foreign state actors to amplify disinformation at a pace and reach often well beyond that of traditional media capabilities.
- As evidenced by the Cambridge Analytica scandal, social media algorithms can allow divisive content to be targeted directly at audiences identified based on personal psychological profiles and prejudices. This can have significant implications for social cohesion when groups that have come together due to mutual prejudice – as an example – have their views reinforced by algorithms that continually suggest material which reinforces such views.
- As far back as 2013, a RAND Corporation research report warned that the internet "increases opportunities for self-radicalisation" because it "acts as an 'echo chamber': a place where individuals find their ideas supported and echoed by other like-minded individuals".[vii]

[vii] Radicalisation in the Digital Era: the use of the internet in 15 cases of terrorism and extremism, Rand Corporation, USA, 2013.

Responses to mitigate the risk posed to Australia's democracy and values, including by the Australian Government and social media platforms

14. The integrity of Australia's democratic systems and processes is essential to maintain public trust in our democratic institutions. Reports of foreign interference in the elections of established democracies around the globe, including through social media platform use, suggests that Australia's electoral events and institutions may be targeted by those seeking to undermine our democratic processes. Foreign actors have demonstrated various motivations for conducting interference using social media platforms – hence it is essential to understand the risks and threats in Australia's unique environment.
15. An Electoral Integrity Assurance Taskforce (the Taskforce) was established to support the integrity of recent Australian electoral events, including the 2019 Federal election and 2018 Federal by-elections. The Taskforce was jointly led by the Australian Electoral Commission (AEC) and the Department of Finance, and included representatives from the Department of the Prime Minister and Cabinet, the then Department of Communications and the Arts (DoCA), the Office of the National Counter Foreign Interference Coordinator (NCFIC) in Home Affairs, the Office of National Intelligence, the Attorney-General's Department (AGD), the Australian Signals Directorate (ASD), the Australian Federal Police (AFP), and the Australian Security Intelligence Organisation (ASIO).
16. Taskforce agencies did not identify foreign interference nor any other interference that compromised the delivery of the 2019 Federal election or would undermine the confidence of the Australian people in the electoral process.
17. In addition to active monitoring of potential instances of interference, Taskforce agencies prioritised the need to have a public media literacy campaign during the election period. The AEC developed and advertised the 'Stop and Consider' campaign on social media, which aimed to increase public awareness of potential disinformation during the election campaign and encouraged people to check the source of information they saw, read or heard.

18. The threat of foreign interference is not just limited to Federal elections. State and territory elections could also be targets for foreign interference activity which could reduce the Australian public's trust in our democratic institutions. Australian Government agencies are actively engaging with relevant state and territory authorities ahead of upcoming elections.

19. The Department of Home Affairs houses a social media insights team that uses publicly available, open-source information to support Australia's social cohesion initiatives by countering violent extremism (CVE) in the online environment. Through the CVE lens, the Department has regularly observed campaigns unfolding on social media that involve disinformation. The Department refers these identified activities to the host platform for investigation and action as possible violations of their terms of service.

20. There is significant variation in each platform's stated position of the issue of 'disinformation', perhaps best exemplified by differences between Facebook and Twitter's stance on political advertising. Whereas Facebook does "not police the truthfulness"[2] of political advertisements on its platform, Twitter has banned political advertising.[3] Such differences also extend to definitions, policies, procedures and responses for dealing with cases of disinformation.

21. The Department has previously observed cases of apparent disinformation on social media platforms that were similar to activities that have been linked by third-parties to foreign state actors. In 2017, following a terrorist attack in Brighton, Melbourne, the Department identified Tweets associated with accounts that have since been publicly attributed by Twitter to a foreign government entity.

22. In another Australian example from 2017, accounts linked to the same foreign government entity were involved in discussions related to a plot to bomb an Etihad airlines flight departing Sydney International Airport. One account used the disrupted plot to promote and amplify the hashtags "#MuslimBan" and "#StopImportingIslam". In this instance, hostile foreign state actors used social media to interfere in Australia's public discourse and attempt to undermine social cohesion.

International policy responses to cyber-enabled foreign interference and misinformation

23. It is important for Australia to continue to engage with, and learn from, other countries in addressing potential foreign threats to our democratic processes through social media. European countries have significant experience and expertise in combatting foreign interference – which they frequently refer to as hybrid threats – through social media, including during recent elections.

24. The European Union (EU) has spent significant resources to support member nations' efforts to combat online disinformation [4]– including establishing a Code of Practice with Google, Facebook and Twitter (Microsoft joined later) in 2018 in the lead up to the EU Parliamentary elections. The European Commission's (EC) formation of the European Centre of Excellence for Countering Hybrid Threats[5] in Helsinki, Finland, has also enabled "nations to come together to share best practices, build capability,[6] test new ideas and exercise defence against hybrid threats."[7]

[2] "Facebook says it won't back down from allowing lies in political ads", The New York Times, 9 Jan 2020, online at: https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html
[3] "https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html
[4] "Tackling Online Disinformation", The European Commission, online at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation
[5] "Hybrid CoE", The European Centre of Excellence for Countering Hybrid Threats, online at: https://www.hybridcoe.fi
[6] "European Disinformation Observatory", Soma Disinformation Observatory, online at: https://www.disinfobservatory.org/
[7] "EU Vs Disinfo", EU vs Disinfo, online at: https://euvsdisinfo.eu/

25. The Swedish Civil Contingencies Agency (MSB) has published a guide on *Countering information influence activities: A handbook for communicators*, which outlines the need to raise awareness across all aspects of society of the challenges of disinformation, social and psychological prejudice, and online deception and bot activity that can threaten democratic activities.[8]

26. The MSB note the damage that information influence activities can have – and highlight the need to safeguard democratic dialogue, identifying that: "the right to open debate, the right to arrive at one's own opinions freely, and the right to free expression—is paramount as we work to lay a solid foundation of social resilience to counter information influence activities." The handbook provides guidance on how communications leads across government can counter information influence campaigns, including through social media.

27. Estonia's Government proudly advertises their reliance on Estonian society's digital literacy levels and confidence in the integrity of their digital systems.[9] Rather than focus on social media, they broaden awareness raising of threats across all digital activities – including trustworthiness of content that is often shared via social media, such as videos and images.

28. The United States and Canada also have significant experience in dealing with online influence campaigns during election campaigns. The US Federal Bureau of Investigation (FBI), Department of Homeland Security and Office of National Intelligence are readily preparing the US public for disinformation campaigns on social media in the lead up to the 2020 Presidential election.[10] The FBI has recommended that voters check the source of information, and "think before they link" online. They also suggest comparing reporting from multiple sources to determine reliable information.[11]

29. The FBI has also established their Protected Voices campaign which includes information about disinformation campaigns on social media platforms that confuse, trick, or upset the public – such as when "a foreign group may purposefully spread false or inconsistent information about an existing social issue to provoke all sides and encourage conflict."[12]

30. The Canadian Government invested in a number of initiatives in the lead up to their 2019 Federal election, including digital media literacy activities to: critically assess online information; understand how algorithms work and when they might impact a user's online experience; recognize how and when malicious actors exploit online platforms; acquire skills to avoid being susceptible to online manipulation; and effectively engage in public debate and online discussions.[13]

31. One example is the Canadian Digital Citizen Initiative, which is a multi-component strategy that aims to support democracy and social cohesion in Canada by building citizens' resilience against online disinformation and building partnerships to support a healthy information ecosystem.[14]

[8] "Countering Information Influence Activities", Swedish Civil Contingencies Agency, online at: https://www.msb.se/RibData/Filer/pdf/28698.pdf
[9] "E-Estonia", E - Estonia, online at: https://e-estonia.com/
[10] "Election Security", Homeland Security, online at: https://www.dhs.gov/topic/election-security
[11] "Joint statement on Election Day preparations", FBI National Press Office, online at: https://www.fbi.gov/news/pressrel/press-releases/joint-statement-on-election-day-preparations
[12] "Combating Foreign Influence", FBI, online at: https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices
[13] "Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation", Government of Canada, online at: https://www.canada.ca/en/canadian-heritage/news/2019/07/helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html
[14] "Online Disinformation", Government of Canada, online at: https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html

32. Australia, together with the international community, recognises that existing international law applies to state conduct in cyberspace, supported by agreed norms of responsible state behaviour. However, some states continue to flout these laws and norms. It is the role of responsible countries such as Australia to ensure there are effective consequences for those who act contrary to this consensus. One example of how Australia has responded to such states in the past is by participating in coordinated efforts with trusted international partners to publicly attribute malicious cyber behaviour to specific nations.
33. Since 2017, Australia has joined international partners on six different occasions to publicly attribute malicious cyber activity to specific nation states. While public attribution is only a successful deterrent for countries that place a high value on their international reputation, and even then may not guarantee behavioural change, it drives public and industry awareness of the inherent risks of our hyper-connected society.
34. The 2020 Cyber Security Strategy will set the foundations for Australia to face the cyber threats of the digital age. It will strengthen our cyber capability, protect the economy, and raise the community's ability to respond to and manage cyber threats. This broader approach will enhance resilience more generally to counter the effectiveness of disinformation campaigns through social media.

The extent of compliance with Australian laws

35. Some examples of Australian legislation regulating social media platforms, include:
    a. ***Privacy Act 1988 (Cth)*** (Privacy Act) which applies to organisations with an annual turnover of more than $3 million and operating in Australia – this includes organisations such as Facebook, Instagram, Twitter, Snapchat and LinkedIn.[15] The personal information shared on such platforms is protected by the data protection obligations under the Privacy Act.
    b. ***Enhancing Online Safety Act 2015 (Cth)*** which establishes a two-tiered scheme for the removal of harassing or abusive material from participating social media services – allowing tier 1 services to participate on a cooperative basis and requiring tier 2 services to comply on a compulsory basis.[16]
    c. ***Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018*** empowers the eSafety Commissioner to issue removal notices that require the providers of social media services, relevant electronic services, designated internet services and hosting services to take all reasonable steps to support the removal of intimate images, or to cease hosting the image.
    d. ***Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth)*** which requires content, internet and hosting providers, including social media platforms, to – within a reasonable time – report to the Australian Federal Police abhorrent violent conduct and remove abhorrent violent material. The Act also provides the eSafety Commissioner the power to notify a service provide that abhorrent violent material is available on their service. 17

[15] "Social media and online privacy", OAIC, online at: https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/social-media/
[16] "Our legislative functions", eSafety Commissioner, online at: https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions
[17] "Abhorrent violent material," the Attorney-General's Department, online at: https://www.ag.gov.au/Crime/Pages/abhorrent-violent-material.aspx

Concluding remarks

36. Foreign interference is a genuine threat to Australia's sovereignty, values and national interests – it can threaten our very way of life. Foreign actors can undermine Australia's sovereignty and advance their interests at our expense by interfering in Australia's decision-making and seeking to unduly influence public perceptions of issues. While social media is only one vector through which foreign interference can occur, social media platforms are unique in their ability to reach billions of people and the reliance on social media as a source of information continues to grow. On that basis, we should anticipate that some foreign state actors will continue to undertake disinformation and foreign interference activities through social media channels.

37. The challenges associated with countering disinformation are likely to grow, as populations around the world continue to engage increasingly through online platforms. Although improved capabilities to identify, attribute and remove disinformation are likely to be an important part of future responses, it will be equally important to raise awareness of disinformation and increase media literacy among the population. The open nature of online platforms means that people are increasingly exposed to a multitude of information sources. Even with improved regulation of the social media sector, assisting individuals to identify 'fake news', better understand the provenance of information and the expertise of the person communicating it, is likely to be important in increasing resilience more generally – both to foreign interference and other types of disinformation.