Australian Government
Australian Security Intelligence Organisation

ASIO submission to the Senate Select Committee on Foreign Interference through Social Media

Inquiry into the risk posed to Australia's democracy by foreign interference through social media

17 February 2023

ASIO

Ref no. PCS 2023-01

Introduction

1. The Australian Security Intelligence Organisation (ASIO) welcomes the opportunity to provide a submission to the Senate Select Committee on Foreign Interference through Social Media.
2. Foreign interference represents a serious threat to Australia's way of life. Clandestine and deceptive interference and espionage activity is pervasive, multifaceted and, if left unchecked, will do serious damage to our sovereignty, values and national interests.
3. Foreign interference is particularly insidious in that it uses our strengths against us. The perpetrators exploit our values, freedoms and trust, thereby undermining our way of life.
4. Social media is a vector for foreign interference, not a threat in and of itself. However, foreign powers seek to do Australia harm through a variety of vectors and capabilities, including social media platforms, often as part of a broader campaign and an invariably integrated one. ASIO, therefore takes an holistic approach to understand, harden against and ultimately counter foreign interference. Our goal is to identify and understand the threats we face, establish a less permissive environment for foreign interference, and work to reduce harm.
5. This submission is divided into 3 parts:
   - Part 1 provides a summary of ASIO's role and accountability framework.
   - Part 2 provides ASIO's definitions of foreign interference and disinformation.
   - Part 3 outlines existing mechanisms for countering foreign interference.

Part 1—ASIO's role and accountability framework

6. ASIO protects Australia and Australians from threats to their security. ASIO's functions are set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). 'Security' is defined in section 4 of the ASIO Act as the protection of Australia and its people from: espionage; sabotage; politically motivated violence; promotion of communal violence; attacks on Australia's defence system; or acts of foreign interference; whether directed from, or committed within, Australia or not; and the protection of Australia's territorial and border integrity from serious threats.
7. The definition of security also extends to the carrying out of Australia's responsibilities to any foreign country in relation to matters noted above.
8. ASIO achieves its purpose by obtaining, correlating, evaluating and communicating intelligence relevant to security. ASIO's anticipatory role means we pursue intelligence which enables the detection of adverse security events at their earliest stage.
9. ASIO must always balance the protection of Australians with the protection of their rights, and welcomes rigorous oversight provided by the Inspector-General of Intelligence and Security—who has powers equivalent to a royal commission—and the Parliament.
10. ASIO is committed to always acting within the letter and the spirit of the law. ASIO ensures our activities are always proportionate to the threat we are confronting and we are using the least intrusive methods possible.

11. ASIO engages fully with its oversight and accountability mechanisms to provide public assurance of the legality and propriety of ASIO's actions.

Part 2—ASIO's Definition of Foreign Interference and Mis/Disinformation

12. The ASIO Act defines foreign interference as:

- Activities relating to Australia that are carried on, by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power, being activities that:
    - are clandestine or deceptive, and:
        - are carried on for intelligence purposes;
        - are carried on for the purpose of affecting political or governmental processes; or
        - are otherwise detrimental to the interests of Australia; or
    - involve a threat to any person.
- A foreign power means: a foreign government; an entity that is directed or controlled by a foreign government or governments; or a foreign political organisation.

13. Foreign interference may include targeting our democratic institutions, political figures, media and community.

14. Disinformation and misinformation share many common attributes, but are distinguished on the basis of intent. Misinformation is generally considered to be false or misleading content spread due to ignorance, error or mistake. Disinformation also involves false or misleading content or misattributing the source of the content, however with an intention to cause harm or deceive. ASIO is particularly focussed on disinformation generated and or spread by, or on behalf of, a foreign actor because of the nefarious intent but notes that the negative effects of the online promulgation of both mis and disinformation can span from having individual or localised impact to broader community and national impacts.

15. For ASIO, the critical question is whether or not the activity, including those conducted on social media platforms, is an act of foreign interference, as defined in the ASIO Act.

- This could include a foreign power, or its proxy, spreading information clandestinely, or with the intention to deceive, to affect Australia's political processes or to be otherwise detrimental to Australian interests. The information could be false, or it could be true but propagated inauthentically.
- Social media platforms popular with some diaspora communities have been used to facilitate interference against groups and individuals. The impact was particularly strong where the platform is controlled by a foreign power, or where there are few platforms able to accommodate foreign language requirements. A further example could be a foreign government covertly spreading misinformation to damage the reputation of an Australian journalist because they published articles critical of that

government.

16. Foreign interference in our political system is different to lobbying, diplomacy or other open and transparent attempts to influence decision-making.

- Publicly praising a foreign regime—even an odious one—is not interference.
- Transparently lobbying on behalf of a foreign government is not interference.
- Diplomacy is not interference. These things are routine acts of statecraft.

17. But any and all of these acts could become foreign interference if they involve the hidden hand of a foreign state. If the person publicly praising another country is doing so because they have covertly received instructions from a foreign power, it could constitute foreign interference if it's detrimental to Australia's interests, or done to affect our political processes.

- Another example of foreign interference targeting our political system could be a foreign power or its proxy covertly directing and controlling the development and distribution of disinformation on a social media platform, aimed at undermining a particular candidate, in a certain electorate, because they were overtly critical of that foreign power.

18. Authoritarian governments are able to direct their country's institutions—including media, businesses and society—to support intelligence or foreign policy objectives in ways which are not acceptable in a democracy. Foreign Powers may also seek to engage in malign influence activities—overt, hostile activities to influence Australia's system of government, government decisions or public opinion, which fall short of ASIO's definition of foreign interference.

- This can create situations where the activities of foreign powers can cause harm to Australia's interests, even without constituting an act of foreign interference.
- This can include coordinated information operations through social media that amplify social disagreement, push political narratives and target specific demographics or individuals within the community. This activity can still cause harm to Australia's national interest and undermine our sovereignty.
- A recent example was where a senior Chinese official posted a fake image of an Australian solider holding a knife to the throat of an Afghan child on Twitter, following the announcement of the findings of the Brereton Report. This was not foreign interference because it was not covert and was overtly attributed to a Chinese government official, but was malign in that it was seeking to portray the Australian Defence Force in a negative light and undermine Australia's contribution to the coalition activities in Afghanistan.

Social Media as a vector for Foreign Interference

19. Social media, in and of itself, is not the threat. Social media, however, provides enormous opportunity for foreign powers seeking to sow disinformation to conduct foreign interference. Social media has benefited from an era of unprecedented connectivity with limited regulation, thus creating the conditions to allow disinformation and misinformation to proliferate and indeed flourish.

20. Many of the deliberate design features of the platforms, such as recommender algorithms, that prioritise content or make personalised content suggestions, or those that allow for anonymity and identity shielding, or have limited content moderation capabilities, can exacerbate the risk of the platform or service being used to conduct foreign interference.

    - In the context of recommender algorithms, a key driver of risk comes from the way a platform or service optimises its recommender systems for greater engagement. If those platforms or services operate an advertising-based business model, they have an incentive to increase user engagement to grow their revenue. This can lead to the promotion of content based on volume of engagement instead of quality and studies show that the more extreme, contentious or hostile the content, the more it is engaged with and this creates significant revenue streams.
    - While anonymity and identity shielding has benefits in that it can protect a users privacy, such as in the case of children to prevent unwanted contact, this feature can be weaponised to enable foreign interference. While some platforms use more rigorous verification processes, which does not necessarily require the service to know or control identifying information of its users, not all do. This allows for fake imposter, impersonator and multiple accounts to be created and operated by one user. This inauthentic use can then be used to conduct online foreign interference activities in an unmoderated way.
    - These features escalate the influence and impact of foreign powers' activities online. The lack of agreed and respected norms and regulations governing social media across the globe, including how safe their design and operating models are, further exacerbates the problem.

21. Foreign powers use of social media campaigns—which can include disinformation and foreign interference—also often defy easy categorisation. Such campaigns are intended to induce changes in the decision making, beliefs and opinions of the target audience. They occur in complex environments where actors overlap, borders are blurred and motives are mixed.

    - There are few laws governing online activity and extraterritoriality of the activity is a challenge. Attribution to a foreign power can be difficult to ascertain, even where such laws come into play.

Case study: Russian foreign interference in the US election[1]

The United States' Office of the Director of National Intelligence (ODNI) assessed that a range of Russian Government organisations conducted influence operations, including on social media, aimed at denigrating a major political party during the US 2020 Federal Elections. ODNI assessed that Russia conducted online influence activities to undermine public trust in the electoral processes and exacerbate social divisions. Russia acted covertly and deceptively by spreading these narratives through social media personas and foreign proxies.

[1] United States National Intelligence Council, Intelligence Community Assessment, *Foreign Threats to the 2020 US Federal Elections,* ICA 2020-00078D.

Part 3 —Existing Mechanisms

22. ASIO and our partners use a suite of measures to disrupt foreign interference plots. The tools include defensive briefings to potential victims; interviews of perpetrators and other targeted intelligence activities; visa cancellations if we are dealing with foreign nationals and law enforcement action.

23. The Counter Foreign Interference Taskforce (CFITF) was established by Government in 2019, and is a multi-agency taskforce designed to mitigate harm and disrupt the threat of espionage and foreign interference by leveraging the unique capabilities of our intelligence and law enforcement agencies.

24. The Taskforce draws on the joint expertise, capabilities and powers of member agencies, co-located in ASIO Headquarters, to boost our ability to discover, investigate, and disrupt espionage and foreign interference.

25. The Taskforce deploys a range of mechanisms to protect Australian interests from foreign interference and espionage, including intelligence operations, law enforcement activity and prosecutions under the Espionage and Foreign Interference Legislation and the Foreign Influence Transparency Scheme, visa cancellations, and financial disruptions.

26. ASIO also has a number of existing channels for clearance holders, members of the public, government organisations, and private sector companies to report concerns about Foreign Interference.

    - Contact reporting is an obligation for all clearance holders. This process is crucial to ASIO's ability to identify hostile intelligence activity, and helping clearance holders and their organisations mitigate risks.

    - ASIO developed the NITRO portal to capture contact reporting from people who do not hold security clearances, but still work on sensitive subjects that could be targeted by hostile foreign powers and their proxies. These people can include, but are not limited to, private industry employees, researchers, academics and former clearance holders.

27. The next Australian federal election is due to be held by June 2025, with other electoral events to occur before then. In the lead-up to these events, we will continue our efforts to harden the threat environment against foreign interference and to disrupt prejudicial activities.

Role of Social Media Platforms and Service Providers

28. Social media platforms and service providers play an important role in addressing this challenge. While ASIO does not lead the policy response, we would support measures that direct social media platforms and service providers, that are or wish to operate in Australia, to remediate design features in their offerings, that enable misinformation and disinformation to be amplified and spread, at volume and scale. Conceptually, this is akin to the accepted concept that technology companies and services are required to remediate known code and misconfiguration vulnerabilities in systems that enable cyber-attacks to occur. Additionally, ASIO would positively support measures that would require platforms and service providers be required to dedicate specific resources to the

identification and moderation of mis and disinformation content, published on their services, commensurate with the volume of content and reach of their services. Meaning trust and safety capabilities continue to be prioritised. ASIO recognises however that any measure allowing digital platforms to respond to misinformation and disinformation need to be balanced with the right to freedom of expression, which is fundamental to our democracy.

Conclusion

29. Solutions to counter the harms from foreign adversary-led disinformation campaigns on social media, given the global nature of the information environment, will necessarily be complex. The means to protect public discourse against foreign interference promoting community harm or political instability, improving the security of the digital landscape and building community resilience to malign influences will almost certainly be multi-faceted and engage interests across the broader community, technology companies, media, regulators and agencies of the National Intelligence Community.

    - It will require building the resilience of the community and our democratic institutions to foreign interference but also broader foreign malign influence.
    - While ASIO's remit includes the protection of Australia and its people from foreign interference, significant harm can also occur through malign influence activity which will require a whole of Government approach.

30. At the request of the Select Committee, ASIO would be pleased to provide a briefing on any of the issues raised in this submission.