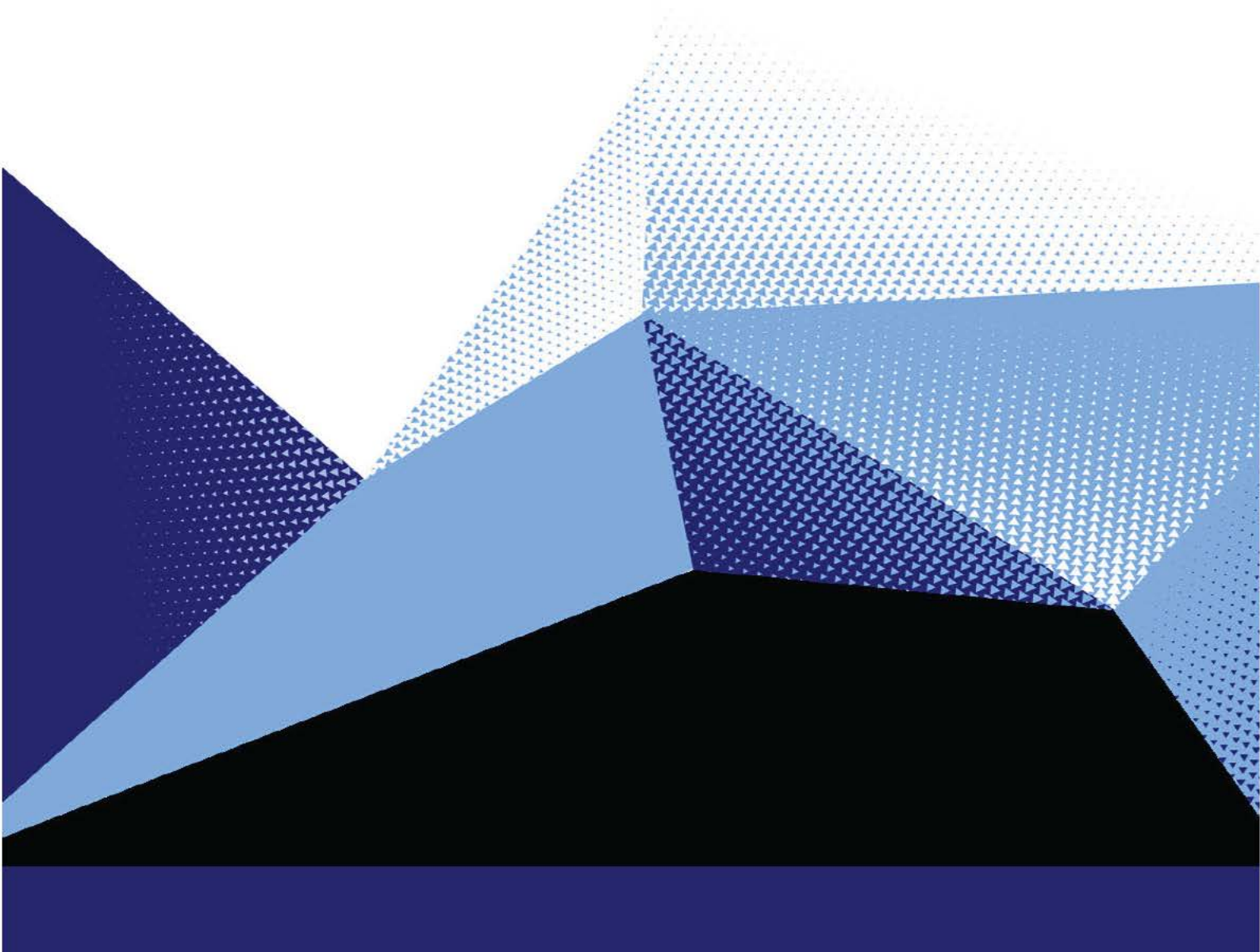
CyberCX

Response to Senate Select Committee on Foreign Interference through Social Media

February 2023



CyberCX

1 Overview

Disinformation and misinformation designed to sow division and doubt is a real and present risk to the Australian way of life.

Disinformation and misinformation are spread through a variety of mediums.

However, the low-to-no barriers to entry combined with minimal consequences of discovery for mal-actors have driven the rise of these platforms as the scalable tool of choice.

These activities have flown under the radar of policy makers for too long; often sidelined as too difficult to reign in, inconsequential, or not worth the effort.

But the implications of the failure to grapple with these forces has become clearer, from our friends in the United States, through to the fledgling democracy in Brazil.

There, as in other places, it has become apparent that disinformation and misinformation need not change the outcome of an election, but merely raise the spectre of illegitimacy.

This is particularly true in Australia, where large and stable majorities commanded by a party of government are less likely to manifest as the electorate fractures away from the major parties. Increasingly, Australian elections are determined by relatively small groups of voters in a handful of marginal seats. In an environment where trust in government is low and falling, claims of "stolen" elections could be easily confected and fuelled.

The risks posed by mis- and disinformation are equally present and growing for the Australian business community, posing questions about what more needs to be done to safeguard and bolster the resilience and potential of ours, the lucky country.

We commend the Committee for their focus and attention to this looming issue.

Our submission is based on CyberCX's significant operational and advisory experience including:

- Insights and research from CyberCX Intelligence, a uniquely Australia and New Zealand focused capability.
- Interviews with our Strategy & Consulting (S&C) and Governance, Risk & Compliance (GRC) experts on how Australia's leading organisations manage cyber-enabled risk, including in relation to social media.
- Being an employer of choice for former intelligence, law enforcement, military and government professionals who wish to continue their work supporting Australia's national interests.

Scope of this inquiry (and our submission)

- Our submission is focused on terms of reference (a) and (b) – namely, on the risk uses of social media pose to Australia's democracy and government responses to this risk.

- While CyberCX sees merit in focusing on the social media dimension of the foreign interference challenge, we urge this Committee to view this dimension within its broader context. Australia's response to cyber-enabled foreign interference must be holistic and effective, regardless of whether the vector is social media.

- In particular, we note that foreign interference campaigns are often multi-stage and multi-platform.
    - An interference campaign communicated via social media may have involved, as precursors, data collection (via various legitimate and illegitimate means), cyber attacks to steal or manipulate information and the curation of networks (online and offline).
    - Interference campaigns on social media often extend to other information spaces, such as clear and dark websites, mainstream media and diplomatic statements.
- We further note that in Australia "foreign interference" is a narrow term, defined in legislation. It does not capture many of the malign foreign influence activities that occur in social media spaces, such as malinformation and disinformation.
    - Throughout our submission, we use the term cyber-enabled interference to generally refer to acts of interference or malign influence that involve a social media dimension.

CyberCX

2 Executive summary

Risks to Australia from foreign interference and malign foreign influence involving social media continue to rise, but government responses have not kept pace with the nature and scale of these risks.

Key risks

Key risks that are currently insufficiently treated in Australia's policy responses include:

1. **Platform power** – a small number of foreign social media companies have significant influence over Australians' access to news and other information and the collection and use of Australians' personal information.

2. **Data breach operations** – foreign governments have rising intent and capability to interfere in democracies by using cyber attacks to steal sensitive information and publish it online, including via social media.

3. **Economic disinformation** – foreign governments have demonstrated an increased willingness to cause economic harm to Australian companies via social media interference campaigns.

Policy response options

To address these key risks, we urge the Australian Government to evolve its response to:

1. **Designate an entity with lead responsibility for whole-of-government efforts to counter cyber-enabled foreign interference**, with appropriate interdepartmental support and collaboration, resources, authorities and a strong public outreach mandate.

2. **Empower citizens and organisations to make risk-based decisions about their own social media use,** by publishing education and guidance material and regular reports and risk advisories on commonly used social media platforms, ensuring this material is accessible for non-English speaking citizens.

3. **Progress robust privacy and data protection reform** to reduce the likelihood and impact of future foreign interference campaigns.

4. **Build capacity to counter social media interference campaigns by supporting independent research** and ensure government has its own appropriate, trusted frameworks for public attribution.

5. **Prefer mandatory compliance and reporting frameworks for social media platforms over voluntary guidelines**, to ensure government – not largely foreign companies – has the final say on managing risks to Australia's democracy.

CyberCX

3 Key risks

Platform power

- Social media platforms exacerbate the risk of foreign interference or malign influence by:
  - Their dominant and largely opaque control over information flows, providing an opportunity for malign foreign actors to manipulate content consumed by Australians, at scale.
  - Collecting and aggregating personal information about millions of Australians, which can be misused to target foreign interference campaigns.
  - Creating communities of users that can be infiltrated or manipulated by malign foreign actors.
- The risk that the dominant position of social media platforms is abused by malign actors is heightened for platforms, such as TikTok and WeChat, which are linked to authoritarian governments. Social media platforms which are owned by Chinese corporations are required by law to cooperate with Chinese government authorities, without the oversight and transparency mechanisms of rule-of-law democracies.

Data breach operations

- CyberCX Intelligence is tracking a rising trend of ***data breach operations*** by nation-state and non-state actors, especially across the US, UK and Europe. Attackers steal – or claim to have stolen – data and publish it online to influence democratic decision-making.
  - Social media is a rich source for data theft and a powerful vector for amplifying stolen information.
  - Australia's spate of high-profile data breaches in 2022 exemplifies the scale and sensitivity of stolen data that could be exploited against Australians in a future targeted foreign interference campaign.
- There is a growing convergence between the state and non-state groups engaged in data breach operations; foreign governments covertly direct, infiltrate or otherwise influence some so-called 'hacktivist' and 'patriotic hacker' groups. This complicates attribution.
  - For example, since February 2022, pro-Russian and pro-Ukrainian non-state groups have intensified use of data breach operations. Operations have been designed to: influence global and domestic public opinion; coerce individuals involved in the war; and to create public fear about the vulnerability of victim countries' networks and data.
- Australia will be most at risk from data breach operations during future diplomatic crises or major political events. For example:
  - In May 2022, CyberCX Intelligence detected a possible campaign to interfere in Australia's federal election, involving emails allegedly stolen from the Nauru Police Force, including some relating to

Australia's offshore processing centres. The stolen emails were published online exactly one week before early voting opened for the 2022 federal election.[1]

- In May 2022, Russian nation-state actors published emails stolen from the accounts of high-profile UK public figures, including a former head of British Secret Intelligence. The emails were published on a disinformation website, which claimed the targeted individuals were part of a conspiracy to interfere in Brexit-related decisions.

Economic disinformation

- Not all cyber-enabled foreign interference has a propaganda effect only. This type of interference can directly harm Australia's economic interests.

- CyberCX Intelligence assesses that several foreign governments have the intent and capability to use social media to harm Australia's economic interests. This could include social media disinformation or data breach operations designed to harm the value or reputation of a company, or to pressure a company or its executives to change their policies or views.

  - For example, in June 2022, cyber security company Mandiant exposed a Chinese Communist Party (CCP) social media information operation targeting Australian mining company Lynas Rare Earths.[2] The campaign included false claims of pollution and called for a boycott. The campaign had minimal impact but indicates the CCP's *intent* to target Australian companies with disinformation to advance China's economic interests.

  - The CCP has a history of targeting private organisations and individuals over policies or statements related to China's human rights record, political system, territorial disputes and position on Taiwan. In October 2019, National Basketball Association (NBA) executive Daryl Morey faced an extensive, orchestrated social media 'trolling' campaign after posting a tweet in support of Hong Kong protesters. This information campaign was accompanied by sustained economic coercion; broadcast bans and lost sponsorship deals in China caused the NBA to lose several hundred million dollars.[3]

[1] https://blog.cybercx.com.au/intelligence-update.-a-question-of-timing-examining-the-circumstances-surrounding-the-nauru-police-force-hack-and-leak
[2] https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies
[3] https://www.wsj.com/articles/china-standoff-cost-the-nba-hundreds-of-millions-11581866522

4 Government responses

The Australian Government's responses have not kept pace with the nature and scale of the risks discussed above. To address this, CyberCX recommends that this Committee consider the following policy options.

Clear direction

The Australian Government should designate an entity with lead responsibility for whole-of-government efforts to counter cyber-enabled foreign interference, with appropriate interdepartmental support and collaboration, resources, authorities and a strong public outreach mandate.

- A single lead entity is needed to coordinate government policy and action on cyber-enabled interference. Importantly, it will also create a clear 'one-stop-shop' for citizens and private sector stakeholders to report, and seek advice about, foreign interference risk linked to social media.
    - We note a similar recommendation was made in the December 2021 Interim Report delivered by the former Senate Select Committee on Foreign Interference through Social Media.
- Current approaches to managing cyber-enabled foreign interference risk are fragmented. For example:
    - In July 2022, the Australian Cyber Security Centre (ACSC) released generic advice for social media users.[4] But this advice focusses on cyber security related concerns, such as identity theft, rather than use of social media for disinformation or other foreign interference acts. It also treats all platforms generically, giving limited insight into differences between them.
    - In September 2022, the Home Affairs Minister is reported to have asked the Department of Home Affairs to review data harvesting by TikTok and other social media platforms. It is unclear whether this review will also look at platforms' content moderation and algorithm practices – another key dimension of the foreign interference challenge.
    - In an election context, while the Australian Electoral Commission is responsible for countering disinformation related to electoral processes, it is doubtful if any department or agency has the capability or authority to lead in relation to a social media disinformation campaign related to political parties, candidates or policies.
- The role, remit and resourcing of the government's National Counter Foreign Interference Coordinator (NCFIC) is unclear, particularly in relation to malign social media influence that falls short of Australia's narrow, legislated definition of "foreign interference".

Empower consumers and organisations to manage risk

The Australian Government should empower citizens and organisations to make risk-based decisions about their own social media use, by publishing education and guidance material and regular reports and

[4] https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-social-media-and-messaging-apps

risk advisories on commonly used social media platforms, ensuring this material is accessible for non-English speaking citizens.

- The information available to Australian citizens regarding foreign interference orchestrated through social media is patchy and generic, despite the key role citizens, the private sector and state and local governments play as vectors and victims of interference.
  - Citizens and private organisations lack the expertise, resources and access to understand the risks of every social media platform they engage with. This problem is exacerbated by the opacity and complexity of platforms' software and terms of service and, in some cases, links with authoritarian governments.
  - For example, the Australian Government has advised federal public servants and politicians of the risks involved in downloading and using TikTok, and a growing number of federal departments have banned the app on work phones. However, most Australian citizens and organisations have not been provided with actionable, specific advice.
- The Australian Government should fill the growing demand for regular, up-to-date research and advice about social media platforms, including:
  - How different social media platforms use and process Australians' personal information.
  - How platforms' algorithms rank, filter and distribute content.
  - Platforms' terms of service and corporate governance policies, including those related to content moderation and oversight.
  - The risks of using social media apps linked to authoritarian governments.
  - Issues related to platforms' cyber security.
- The Australian Government should also consider providing education and guidance materials about social media interference, such as:
  - How users can identify misinformation, malinformation and disinformation.
  - How users can protect themselves against interference on social media.
- This information needs to be specific to commonly used platforms, regularly updated and actionable. It may be useful to report against a consistent framework for every platform, identifying their respective strengths and key areas of foreign interference risk.

Progress robust data protection reform

The Australian Government should progress robust privacy and data protection reform to reduce the likelihood and impact of future foreign interference campaigns.

- CyberCX welcomes the government's decision to accelerate privacy law reform and urges the government to use this reform agenda to reduce vectors for foreign interference.

- A strengthened, more transparent regime for the collection, storage, use and security of personal information can reduce the likelihood and effectiveness of targeted social media disinformation campaigns and data breach operations.

Expose foreign interference

The Australian Government should build capacity to counter social media interference campaigns by supporting independent research and ensure it has appropriate, trusted frameworks for public attribution.

- To date, revelations about cyber-enabled interference risk or specific campaigns in Australia have largely been made by think tanks and private sector organisations, on an ad hoc basis. These issues are not consistently or capably monitored and publicly disclosed.

- The Australian Government's own approach to attribution social media interference and malign influence is unclear, with different Ministers discussing foreign disinformation using varied formats and points of evidence.

  - For example, in 2020, the then Foreign Minister referred to an attribution by the European Commission that Russia and China had engaged in targeted disinformation related to Covid-19, and reiterated an attribution by Twitter that Russia, China and Turkey had engaged in information operations on Twitter's platform.[5] However, there are few instances of Australia directly attributing cyber-enabled interference campaigns to foreign actors.

- In other peer democracies, independent think tanks, researchers and private corporations play a greater role in investigating, exposing and analysing social media interference and malign influence. The Australian Government could facilitate more research by independent, apolitical and trusted organisations by:

  - Providing grants to academic and private sector organisations for social media monitoring and investigations.

  - Bolstering laws related to platform disclosure, so that researchers can access more, higher-quality information about cyber-enabled interference precursors and activities.

Move beyond voluntary guidance for social media platforms

The Australian Government should prefer mandatory compliance and reporting frameworks for social media platforms over voluntary guidelines, to ensure government – not largely foreign companies – has the final say on managing risks to Australia's democracy.

- Australia is well-positioned to lead globally on the regulation of foreign interference risk via social media.

  - The Australian Government has played a leading role among democracies in its legislative and policy response to foreign interference, from 2017. It has also been a pioneer in digital platform

[5] https://www.foreignminister.gov.au/minister/marise-payne/speech/australia-and-world-time-covid-19

regulation, most recently for example via the *News Media and Digital Platforms Mandatory Bargaining Code* introduced in 2021 and the *Reducing Scam Calls and Scam SMS Industry Code* introduced in 2022.

- Currently, how social media companies identify, disclose and address foreign interference risk on their platforms is inconsistent and ad hoc.
    - Even where platforms have developed counter-interference or counter-disinformation frameworks, there is no guarantee these will be maintained or enforced – they are susceptible to changes in corporate direction or leadership.
- To ensure governments, researchers and wider society has access to information about social media platforms and foreign interference risk, the government should ensure it has appropriate authorities and mandate to require social media companies to provide consistent, high-quality reporting and to sanction non-compliance.

5 Further information

CyberCX would welcome the opportunity to engage with the Committee further on these issues. For further information, please contact us directly:

Katherine Mansted
Director—Cyber Intelligence and Public Policy

Megan Lane
Director—Communications and Government Affairs

About CyberCX

CyberCX is the largest and leading provider of cyber security services organisation in Australia. With a workforce of over 1,300 cyber security professionals, CyberCX is a trusted partner to the private and public sectors, helping customers confidently manage cyber risk, respond to incidents, and build resilience in an increasingly complex and challenging threat environment.

CyberCX provides end-to-end cyber capabilities, enabling customers to securely accelerate their digital transformation strategies.

CyberCX's services include consulting and advisory, governance, risk and compliance, incident response, security testing and assurance, network integration and security, cloud security and solutions, identity and access management, managed security services and cyber security training.