AP4D
Asia-Pacific Development, Diplomacy & Defence Dialogue

Options Paper

What does it look like for Australia to...

Use All Tools of Statecraft in the Information Environment

SUPPORTED BY

Australian Government
Australian Civil-Military Centre

Asia-Pacific Development, Diplomacy & Defence Dialogue

Secretariat@asiapacific4d.com

www.asiapacific4d.com

@AsiaPacific4D

https://au.linkedin.com/company/asia-pacific-development-diplomacy-defence-dialogue

https://www.youtube.com/@Asia-Pacific4d

You can cite this paper as: Asia-Pacific Development, Diplomacy & Defence Dialogue, What Does it Look Like for Australia to Use All Tools of Statecraft in the Information Environment (Canberra 2024): www.asiapacific4d.com

First published April 2024

ISBN: 978-0-6458800-9-0 (online)

ISBN: 978-0-6458800-8-3 (print)

DISCLAIMER

Executive Summary

The global information environment is part of modern Australian political, economic and social life, bringing with it new kinds of connectivity and opportunity. At the same time, it is a vector for serious threats to Australia's national interests, such as foreign interference in the country's democratic political system, as well as to global stability more broadly.

Coordinated disinformation campaigns are now an established feature of domestic politics in Australia's region. This means that attempts to mitigate harms in the information domain are now at the top of political and security agendas, both for Australia and for partners and allies. This is particularly pertinent in a year with a rapid succession of elections around the world.

Emerging technologies continue to shape the information environment in new ways, with advances in artificial intelligence both enabling the faster detection of information operations, but also making the creation and dissemination of disinformation and propaganda cheaper and more convincing.

Compounding these vulnerabilities is the existing low level of public literacy on threats in the information environment and a lack of easy-to-use information and services to empower individuals and groups to protect themselves from harm.

Australia has undertaken a range of measures to manage risks in the information environment – often being a first mover in this space – but these have not been enough to stem the tide.

Australia should commit to taking a leading role in promoting a healthy information environment regionally and globally.

Given the porous, globally networked nature of the information environment – and the power and concentration of companies that control the major global information platforms – a multilateral approach to the building of new norms and standards in the digital age is an urgent priority. Australia should position itself to be an influential participant in these debates.

Australia should clearly articulate rights and responsibilities around information and actively promote these domestically, in the region and internationally, including through resilient information infrastructure. At home, Australia should develop a comprehensive and enforceable framework of legislation grounded in liberal democratic values to constrain harmful actors and encourage good-faith activities in the information environment. Internationally, promoting a truth-based information environment should be part of Australia's development and diplomatic partnerships, making this a centrepiece of Australia's brand abroad.

Australia's objectives in the information environment should not just be defined by threats or hazards, but by a positive vision of what Australia wants in relation to security, prosperity, sovereignty, rule of law, equality and freedoms. Such objectives should be organised around the following themes:

- protecting and empowering citizens
- improving trust in the information environment
- protecting the function of democratic institutions and the democratic process
- developing a proactive and strategic approach to the information environment that clearly articulates a vision for an information ecosystem that works in Australia's national and public interest

The pursuit of this vision will require a whole-of-nation effort, recognising that much of Australia's information power comes from the non-government cultural, social and economic spheres. An all tools of statecraft approach is needed to maximise Australia's influence in the information domain to shape a healthy information environment.

This paper suggests the following pathways for Australia to use all tools of statecraft in the information environment:

- Establish a national body for the information environment to coordinate work across government and engage in dialogue with non-government actors such as industry, civil society, non-governmental organisations and academics
- Increase resourcing for professional standards bodies
- Strengthen regulation and oversight of social media platforms
- Ensure government has the power and data to investigate breaches
- Provide tangible and rapid support to Australian diasporas targeted by disinformation and harassment by malicious actors
- Commit to a long-term public campaign supporting truth-based communication and the inclusion of digital media literacy in education curriculums
- Support civil society organisations advocating for digital rights and improving access to justice for online harms
- Support fact-checking organisations operating at arm's length from government, such as by requiring social media platforms to fund fact-checkers in the countries they operate
- Focus on pre-bunking (pre-emptively debunking) by predicting disinformation narratives and proactively seeding truthful framing of events
- Support a strong, diverse public interest journalism sector through legislation and incentives
- Work with allies and partners to promote a healthy global information environment, including legal and financial sanctions against enablers of disinformation, online exploitation and human rights abuses
- Develop a system of governance support to help countries deal with disinformation during election cycles
- Support partners to develop and maintain resilient information infrastructure, including alternative information pathways where access is unavailable
- Urgently increase investment in Indo-Pacific media, including supporting journalism training, wages, professional bodies, disinformation observatories and co-production.

WHAT IS THE INFORMATION ENVIRONMENT?

The "information environment" or "information ecosystem" is a socio-political space in which information is created, stored and exchanged (including in the form of data/knowledge/intelligence) between individuals, organisations and governments (including information exchanged between humans, humans and non-humans, machines-and-humans and machine-to-machine). A democratic information environment needs to privilege accurate information and to encourage shared understanding.

WHAT IS DISINFORMATION AND MISINFORMATION?[1]

- **misinformation:** false, incomplete, or misleading information that is shared without malicious intent
- malinformation: when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere
- **disinformation:** verifiably false or misleading information that is created, presented and disseminated for economic gain or with intention to cause harm (including threats to democratic, political and policymaking processes as well as public goods such as the protection of citizens' health, the environment or security)

WHAT IS INFORMATION WARFARE?

- **information domain:** comprises the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organisations, and systems that collect, process, disseminate, or use information. Operations in the information domain seek to change the behaviour of a target by generating effects upon one or more of these factors.
- **information warfare:** the acquisition, management, and use of information and information systems in a national military strategy targeted to weaken an adversary information systems while protecting a nation's own information systems from harm.
- **information operations:** coordinated activities to generate strategic effects through the information domain, typically involving the production and dissemination of targeted information.
- **information power:** the capacity for a state to acquire, manage and leverage information and information systems to advance its national interests.

Note: These definitions are offered for the purpose of this paper only. There is a high level of confusion and misappropriation of these terms in public debate with many used interchangeably.

Defining these terms for legislative purposes has become highly politicised, with the danger of government definitions of disinformation potentially impinging on rights to freedom of speech. On the other hand, lack of a definition makes enforcement of disinformation legislation very difficult to prosecute. In the UK, to get around this challenge, law makers used legislation that clearly targets highly coordinated mass dissemination of disinformation on social media platforms. In the European Commission's legislative framework on disinformation, lawmakers are experimenting with a dynamic concept of disinformation to guide enforcement so that the Commission can change definitions to keep up with the emergence of new disinformation trends.

1 Adapted from Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making", Council of Europe, September 2017, https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

Why it Matters

The global information environment transcends Australian political, economic and social life, bringing with it new kinds of connectivity and opportunity. It is also a vector for serious threats to Australia's national interests, Australia's democratic political system and to global stability more broadly. While the information environment is not new, evolving tactics, technologies and techniques to generate effects in the information domain are being utilised by authoritarian actors, driving malign information operations and hybrid warfare strategies across the global system.

This has led the Australian government to introduce a suite of foreign interference legislation in recent years,[2] aimed at countering these and other types of influence operations. The trend lines are likely to worsen in the next five years – particularly in the next 12 months with a rapid succession of elections around the world[3] – as disinformation becomes embedded in political cultures both in Australia and abroad, and with the advent of ever more advanced generative artificial intelligence (AI) technology.

There is a clear need for Australia to continue to enhance and refine its approach to the information environment across all tools of statecraft to enable it to fully take advantage of the opportunities and effectively understand, pre-empt and respond to the threats.

Attempts to mitigate harms in the information domain are now at the top of the political and security agenda of Australia's partners and allies. Given the globally networked nature of the information environment, and the power and concentration of companies that control the major global information platforms, a multilateral approach to the building of new norms in the digital AI age is becoming both an urgent priority and one that may only be tackled with international coordination.

These modes of warfare and influence exploit all forms of communication. Methods can be campaigns that span cyber activities, disinformation, foreign interference, market manipulation, surveillance and theft of sensitive data and intellectual property.

It is important to note that campaigns in the information domain are often accompanied by other enabling factors. Examples include dark money networks and systematic long-term attempts to cultivate influence with political and economic elites in target countries. Economic coercion can also be a feature, as can attempts to supress accurate reporting and analysis by the targeting of journalists, academics and civil society leaders, both via online and real-life threats. State control of underlying digital infrastructure also provides the means to synchronise information operations to support malicious activities in other domains, including warfare.

The efficacy of these methods are all likely to be further boosted by the 2023 release of Large Language Learning Model AI technologies, with very few guardrails. These new technologies are making the creation and dissemination of disinformation and propaganda much cheaper, easier, accessible and more convincing.[4]

AI has the potential to be a significant contributor within the information environment, contributing to information systems and supplementing decision making. AI will present new options for rapidly detecting falsified information and digital behaviour that is indicative of deliberate information operations. However significant issues remain around the verifiability of information produced by AI, it being able to create false digital content of greater quality and in greater volumes than in the past. At the time of writing, it is estimated that around 1% of information on the internet is produced purely by AI technologies but this figure is likely to grow exponentially, adding to the total of inaccurate information online.

2 Department of Home Affairs, "Countering foreign interference", https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

3 Kat Duffy and Katie Harbath, "Defending the Year of Democracy", Foreign Affairs, January 2024, https://www.foreignaffairs.com/united-states/defending-year-democracy

4 Allie Funk, Adrian Shahbaz and Kian Vesteinsson, "Freedom on the Net 2023: The Repressive Power of Artificial Intelligence", Freedom House, 2023 https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence#generative-ai-supercharges-disinformation

At the same time, the English language news industry continues to lurch from crisis to crisis. The business model of news first came undone with the migration of advertising to online platforms. But various fixes, from subscription-based models, to charging social media platforms for the use of news content have been unravelling over the last 12 months. Major global mast heads like the Washington Post, the Wall Street Journal and the LA Times have haemorrhaged staff in recent months, and Meta has announced the end of its payment for news content arrangements in Australia as well as the removal of news tabs on their platforms. It has been reported that this move by Meta will take approximately AUD $70 million out of commercial news and public broadcasting.

In Australia's immediate region, malicious information operations have been proliferating. For example, coordinated disinformation campaigns are now an established feature of domestic politics in Southeast Asia, as well as being used as a tool of strategic influence in the region.[5]

In the Pacific, nations have been subject to disinformation on issues such as COVID-19, which harmed public health responses to the pandemic. But some political leaders have also begun to look to authoritarian methods of information control, such as the use disinformation and the suppression of press freedom in order to maintain their hold on power, with negative consequences for democracy and stability.

Coordinated disinformation campaigns have grown in intensity, affecting many areas of Australian public life. Of particular concern is the growth of disinformation groups in Australia. This includes threats to public health via the spread of disinformation around COVID-19 vaccination; the targeting of Australian public servants, as evidenced by unprecedented threats of violence against Australian Electoral Commission in recent elections and the Voice Referendum; well-funded disinformation campaigns against action to mitigate carbon emissions; and the mainstreaming of disinformation as tool of political campaigning.

"Cyber is no longer a technical topic but a whole-of-nation effort."

"Australia will deploy all arms of statecraft to deter and respond to malicious cyber actors."

2023-2030 Australian Cyber Security Strategy

"New and emerging technologies continue to alter our world in profound and unpredictable ways. Advanced manufacturing, artificial intelligence and other technologies are transforming workforces. New jobs will be created and old jobs lost, generating demand for education and upskilling. Technologies that increase human connectivity will require strong safeguards to reduce risks such as foreign interference, disinformation, loss of privacy, and infringements upon individual security, rights, and freedoms. Strong, effective leadership from governments, the private sector and civil society is needed to tackle complex structural reform."

Australia's International Development Policy

5 Anastasia Kapetas, "Southeast Asia on the forefront of disinformation for profit and power", The Strategist, May 2021, https://www.aspistrategist.org.au/southeast-asia-on-the-forefront-of-disinformation-for-profit-and-power/

Regulatory and civil society efforts to counter threats in the information environment have succeeded in raising awareness about single issues, such as disinformation or cyber security. But they have largely failed to halt the political and security risks flowing from an evolving information domain and increasingly coordinated campaigns by harmful actors, for example discussions about the regulation of new artificial intelligence is only just beginning whereas AI is already in use in disinformation and cyber activities. This prompts urgent questions about what steps can be taken to address these risks in a coordinated manner.

New and much more ambitious regulatory, legislative and legal efforts in the EU and the US have emerged over the last two years which attempt to counter information domain harms at the national, regional and global level. The urgency of these efforts has been driven by Russia's invasion of Ukraine, and the political success of a radicalised far right in US and EU. Weaponised disinformation and propaganda are critical tools for these actors and often connect political movements across national borders.

In Australia, efforts to counter malicious information operations, disinformation and other threats in the information domain have been piecemeal and reactive, rather than comprehensive and strategic. This perhaps reflects a view that disorder in the information environment is a "social media issue", rather than a structural crisis. It may also reflect a feeling of powerlessness on the part of lawmakers in the face of globally powerful digital media platforms, a lack of technological and conceptual literacy, and confusion about what constitutes free speech in a democracy.

What is missing is a consistent, positive, publicly articulated discussion about the kind of information environment Australia wants that leads to a vision for what would work best for Australia's democratic national interests and regional and global stability. This paper outlines what such a vision would look like and how Australia might use its tools of statecraft to holistically pursue that vision.

An all tools of statecraft approach[6] is needed to maximise Australia's influence in the information domain and its ability to proactively shape a more transparent and credible information environment.

A truth-based information system is a fundamental nation and global public good, needed for basic governance in any political system. Especially in democratic systems, it is needed to secure the rights of citizens, for economic prosperity and as a deterrent to corruption and foreign interference. Australia needs an innovative and truth-based information ecosystem to address multiplying domestic and systemic global challenges, including the expansion of revisionism, extremism and authoritarianism, as well as existential global commons issues arising from climate change.

Information environment issues are right at the top of the international agenda and intersect with every other major threat. Australia should position itself be an influential participant in these debates.

6 AP4D, What does it look like for Australia to use all tools of statecraft in practice (Canberra 2023), https://asiapacific4d.com/idea/all-tools-of-statecraft/

Perspectives

EXISTING MEASURES

Australia has already undertaken a range of measures to manage the information environment, which include:

- Expanding the role and funding of the Office of the eSafety Commissioner.[7]
- Targeting unfair commercial practices of social media platforms through the Australian Competition & Consumer Commission (ACCC).
- Implementing a media bargaining code.[8]
- The establishment of the National Counter Foreign Interference Coordinator, the Counter Foreign Interference Taskforce, the Electoral Integrity Assurance Taskforce and the University Foreign Interference Taskforce.[9]
- Establishment of a disinformation taskforce in the Department of Foreign Affairs and Trade (DFAT).[10]
- Introducing offences under the Criminal Code Act 1995 and new regulations in the Online Safety Act as part of commitments to the Christchurch Call initiative.[11]
- Developing a voluntary code of conduct for social media platforms, monitored by the Australian Communications and Media Authority (ACMA).[12]
- Working with social media platforms to take down coordinated disinformation networks.
- Small Commonwealth grants to promote local news in Australia's regional areas.[13]
- Increased funding to the Australian Broadcasting Corporation.[14]
- Experimentation with public literacy campaigns on disinformation.
- Attempts to develop anti-disinformation legislation that is enforceable and carries more severe penalties. The latest attempt by the government has generated a high degree of controversy.[15]
- Funding journalism initiatives in the Pacific.[16]
- Developing a National Cyber Security Strategy.[17]
- More comprehensive legislation around cyber security, including giving the federal government power to compel companies to cooperate where national security is at stake.
- Strengthening legislation and activities to counter foreign interference.
- Classified capabilities in national security agencies.
- A proposed amendment to the Defence Act, known as the Safeguarding Australia's Military Secrets Bill, to require certain former Australian Defence Force members and Defence employees to obtain authorisation if they intend to work for a foreign military, foreign government or foreign government entity.
- Artificial intelligence codes of conduct.

These efforts are welcome steps and Australia has often been a first mover in this space – as, for example, with negotiating with online platforms to pay for news.

7 https://minister.infrastructure.gov.au/rowland/media-release/budget-2023-24-connecting-informing-and-protecting-australians#:~:text=The%20Albanese%20Government%20will%20quadruple,safer%20experience%20online%20for%20Australians.

8 https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/government-implement-all-recommendations-news-media#:~:text=The%20Code%20is%20intended%20to,under%20the%20Code's%20designation%20provisions.

9 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/overview

10 https://www.themandarin.com.au/135202-dfat-to-set-up-disinformation-taskforce/

11 https://www.christchurchcall.com/assets/Documents/Christchurch-Call-Community-Statements-2022.pdf

12 https://www.acma.gov.au/report-digital-platforms-efforts-under-australian-code-practice-disinformation-and-misinformation

13 https://www.infrastructure.gov.au/department/media/news/grants-open-support-regional-and-local-newspapers

14 https://www.publicmediaalliance.org/abc-receives-funding-boost/

15 https://www.theguardian.com/australia-news/2023/nov/13/labor-misinformation-bill-objections-freedom-of-speech-religious-freedom

16 https://www.dfat.gov.au/geo/pacific/people-connections/media-partnerships-in-the-pacific#:~:text=Australia's%20Pacific%20Media%20Assistance%20Scheme%20(PACMAS)&text=PACMAS%20is%20implemented%20by%20ABC,and%20professional%20Pacific%20media%20sector.

17 https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

This paper is the culmination of five months of consultations with some of Australia's foremost experts on information and communications practices.

The process commenced with a dialogue event in August 2023 and was led by a working group of experts drawn from academia, journalism, public policy and the non-government sector. AP4D also gathered perspectives from a group consultation with the Australia Asia Pacific Media Initiative and from individual consultations.

This paper is a synthesis of these contributions.

AP4D is grateful to those who have contributed to the development of this paper. Views expressed here cannot be attributed to any individuals or organisations involved in the process.

A full list of individuals and organisations consulted can be found at the end of the paper.

THREATS IN THE INFORMATION ENVIRONMENT

There was broad agreement on the nature of threats that Australia is facing in the information environment, but some differences over which threats are considered the most urgent. Those consulted agreed that these threats were fast moving and protean in nature, thwarting purely legislative responses which tend to be slow moving.

Most of those consulted thought that **disinformation** was the most urgent threat in the information environment, noting that this harm is intertwined with other threats such as cybercrime, data privacy and online exploitation. Participants also noted that most of the key threats are interconnected.

Compounding these vulnerabilities is the existing **low levels of public literacy on threats** in information environment, and insufficient and easy-to-use information and services that empowers individuals and groups to protect themselves from harms.

From a national security perspective, there is a serious threat that foreign countries use information warfare techniques to **erode Australia's multicultural identity and social cohesion** and to promote political and economic elites that are friendly to their economic and political objectives. In this, of course, Australia is not alone. These are global trends.

Targeting of diasporas in Australia through information technologies is also an issue. Both great powers and a host of other smaller countries have used disinformation, propaganda, online and direct intimidation of Australian immigrants to control the views of diasporas in Australia and to prevent these diasporas from nurturing dissident movements.

Information domain threats are accelerating the **deterioration of Australia's broader security environment**. At the global level, Australia, like many other middle powers, draws its security from the institutionalisation of norms outlawing most forms of state-based conflict and promoting multilateral cooperation on economic, security and human rights issues. Those consulted described the fragility of many of the multilateral institutions Australia has depended upon for its security, freedom and prosperity, sometimes referred to in shorthand as the "rules-based international order". One participant noted that at the 2024 World Economic Forum, restoration of trust in societies was the key issue on many panels. Also much discussed was the fragility of the international environment in 2024, with many elections in which interference, including through disinformation can be expected, compounded by climate change, conflict and new AI technologies might exacerbate these structural crises.

A key goal for **malign authoritarian actors** is to destroy those norms by leveraging the global information ecosystem to encourage social and political fractures in democratic nations and to support the success of radical political movements that share their worldviews.

A parallel goal of some authoritarian actors is to promote their **style of information governance** across Africa, Asia, the Pacific and South America, and build anti-western alliances. Norm-shaping is a key tool here also: nominally democratic countries are promoting legislation aimed at suppressing press freedom, political opposition, dissent and protest. They often seek communications infrastructure and capabilities that support state surveillance and content control.

Consultees discussed the **radicalisation** of sections of the Australian population towards political violence in support of authoritarian, far-right, white supremacist, misogynistic and anti-government agendas. These groups have gained strength in Australia using online disinformation, propaganda and hate speech as potent recruitment tools. The Australian Security Intelligence Organisation (ASIO) and other Australian law enforcement bodies consider these groups to be Australia's largest and fastest-growing terrorist threat.

> "Australia and other countries must also deal with challenges from efforts to interfere in democratic decision-making and to shape public opinion through misinformation, including through the use of new technologies… Our strategies in response must be long-term and flexible. We will need to safeguard community cohesion and the resilience of our society."
>
> *2017 Foreign Policy White Paper*

Those consulted focused on the power and influence of **multinational social media and information technology companies** and their resistance to regulation and oversight. Most disinformation is delivered via these platforms, and their business models depend on generating maximum engagement through content engineered to cause shock and outrage. The speed of dissemination means that disinformation can quickly affect a political system and be very difficult to counter. Perceptions are that platform owners have paid lip service to content moderation, but studies have shown that only a tiny fraction of disinformation disseminated via coordinated networks is taken down. Some platform CEOs have also recently shown a propensity to actively promote hate speech, conspiracy theories and disinformation.

The above is illustrative of a deep decline in information sovereignty - the increasing dependence of countries like Australia on a handful of global companies that operate global information infrastructure monopolies in social media, data, AI, satellite technology and cloud computing, and therefore Australia's critical infrastructure, and the inability of nations to direct their own digital technology course, for defence, economic or social purposes.[18]

Generative artificial intelligence (AI) is supercharging harmful information operations and activities. These technologies enable much more credible image, audio and text based deep fakes, an increased ability to create and automate fake accounts and the ability to create news sites that effectively mimic credible news sources. These tools have been embraced by state-based disinformation networks, as well as driving outsourcing of coordinated disinformation networks to the private sector.

Participants noted that newsrooms are already struggling with finding images that have been digitally altered, and the volumes are only likely to increase. Newsrooms need support here, through either tech fixes or a government funded body that helps journalists with best practice, and that can be widely shared through media and government networks.

18 Linton Besser, "The Voice campaign was infected with disinformation. Who's in charge of inoculating Australians against lies?", ABC News, October 2023, https://www.abc.net.au/news/2023-10-17/voice-referendum-infected-disinformation-australians-lies/102981108

The embrace of disinformation by **organised criminal networks** means that Australian citizens are subject to an increasing number of online scams, fraud, identity theft and exploitation. The manifold economic issues flowing from disinformation include low trust in email and text communications from companies as well as declining trust in government institutions.

The increasing use of AI also brings many threats to businesses. Audio and visual deep fakes make **identity theft and fraud** much easier. The temptation to completely automate customer service at every level using increasingly sophisticated AIs may cause severe reputational harm. Chatbots have no accountability in themselves, and accountability is the essence of a trusted relationship. The same also applies to the automation of government services, as exemplified by the Robodebt scandal in Australia, and the UK Postal Service scandal.

Consultees expressed the view that in the **Pacific**, the information environment is becoming increasingly captured – especially by Chinese influence – and that independent public interest media is facing existential threats. With core central news services are facing financial and staffing crises, Pacific media experts say that the fate of public interest media here will be decided in the next five years.

> "Information underpins all effective military operations. Secure and resilient information systems are critical to delivering capability, conducting operations, sharing information with partners and communicating with other government agencies. This includes measures to ensure that critical information and communications infrastructure, systems and networks are defended against cyber attacks."
>
> *2020 Defence Strategic Update*

OBJECTIVES AND OPPORTUNITIES FOR AUSTRALIA

Participants agreed that Australia's objectives in the information environment could be organised around the following themes:

- protecting and empowering citizens
- improving trust in the information environment
- protecting the function of democratic institutions and the democratic process and
- developing a proactive and strategic approach to the information environment that clearly articulates a vision for an information ecosystem that works in Australia's national and public interest

This is required both domestically, regionally and globally and includes partnering with other countries to promote international norms to stabilise a deteriorating global information environment.

A common view from participants was that Australia's objectives in the information environment should not just be defined by threats or hazards, but by a positive vision of what the nation wants in relation to security, prosperity, sovereignty, rule of law, equality and freedoms. Once it is decided what this would look like, the next step would be to craft policies to support that vision while managing and mitigating the hazards and threats.

Australia should first recognise the centrality of this issue to its national interests. This means acknowledging that the deterioration of the information environment is at the top of the global political and economic agenda. Many of our allies and partners see this issue as existential, meaning that Australia has the opportunity to work together with like-minded countries to ensure that the information environment remains truth based.

This is an urgent foreign policy priority. This constant weaponising of the information environment is not sustainable, and so Australia needs to work with partners on a kind of information 'disarmament'.[19]

19 Nicholas Cull, Reputational Security: Refocusing Public Diplomacy for a Dangerous World (Wiley, December 2023)

WHO ARE THE KEY ACTORS AND STAKEHOLDERS IN THE INFORMATION SPACE?

GOVERNMENT

- Government departments and agencies (federal, state & territory)
- Military & intelligence agencies
- Legal institutions
- Media standard setting
- Regulatory bodies
- Law enforcement
- Cyber capabilities
- Public communications

PRIVATE SECTOR

- Corporations
- AI platforms
- Data companies
- Creative industries
- Spam companies
- PR/advertising political advisory agencies
- Block chain/crypto companies, white and black
- Gaming platforms
- Cyber security firms
- Secondary communication systems (in case of social media failure)

NON-PROFIT

- Open-source intelligence
- Think tanks
- Civil society groups
- Universities
- Education institutions
- International NGOs
- Multilateral institutions
- Research organisations (digital tech)
- Fact checkers
- Religious institutions and organisations
- Wikipedia
- Educators, media literacy organisations, libraries
- Sporting organisations
- Sporting institutions
- Political parties

TRADITIONAL MEDIA

- Traditional media companies
- Public broadcasting institutions
- Newsrooms

NEW MEDIA

- Social media platforms
- Browser platforms
- Encrypted messaging platforms
- Dark web
- Longer form content platforms
- Message boards
- Bot farms

MALIGN ACTORS

- Hackers
- Mercenary groups
- Terror groups
- Hostile foreign states and their corporate proxies
- Social media influencers who derive profit from pushing disinformation narratives

INDIVIDUALS

- Publics (different generational and demographic audiences)
- Influencer networks
- Powerful individual influencers
- Celebrities

Australia also needs to make sure that it does not succumb to disinformation at home. When democracies use disinformation at home it undermines trust globally. National reputation management becomes much more difficult in a global information environment that authoritarian actors use to propagate vast amounts of propaganda and disinformation to destabilise the global system.

In this effort, Australia does not need to take an anti-technology stance. Rather, the government can affirm that there have been huge innovations on the technical side which now need to be matched by social and legal innovations – and aim to become a leader in public policy for technology that directs it towards the democratic public interest. This means actively supporting the uses of digital technologies to support social cohesion, economic prosperity, the rule of law, human rights and a trusted public square.

Australia should commit more resources to protecting citizens from harms in the information environment such as disinformation, foreign interference, identity theft, surveillance, and exploitation, through long-term well-funded and ongoing public literacy campaigns that are designed to reach diverse audiences. These campaigns should empower citizens to discern the accuracy of the information they see online, to encourage the promotion of accurate information in information systems, and to protect citizens from exploitation through information systems, including using appropriate reporting and assistance mechanisms.

Any literacy campaigns need to engage citizens, incorporate a diversity of voices, especially among younger demographics. Part of this is really articulating the role of free speech in our society, consulting broadly and deeply with citizens on what this means in a democracy in a digital age of accelerated AI technologies.

There is also an urgent need to build literacy in Australia's bureaucracy on information environment threats and building better strategic communication skills in departments.

Australia also needs to consider the role of citizens in shaping new artificial intelligence (AI) technologies. Human centred AI is a buzzword, and companies like Open AI have relied on open-source development to move the technology along. But there is a huge asymmetry here between AI companies and citizens.

This asymmetry prompts urgent questions about letting a very narrow subset of society, namely tech developers, set the direction for these increasingly powerful technologies with very little input from the rest of society, whose lives will be most deeply impacted. So how might these new tools be shaped to serve a democratic public interest? Without grappling with these questions, it will be very difficult to build public trust in AI as synthetically generated information grows and AI is used to support increasingly complex decision making.

Australia needs to cultivate an information environment where calm and deliberative thinking is encouraged. Online social media communication has been often described as an outrage machine, promoting extreme emotional reaction and polarizing content. Australia needs to find a way to counter these effects as deliberative thinking is critical to maintaining perspective, empathy with the experience of others, and building healthy social connection.

Australia also needs to use the existing information environment much more proactively. To develop a clear sense of our international strategic communication objectives that arise from Australia's role as a democracy in the region.

There especially needs to have a clear information strategy that projects our core narratives, that strengthens relationships with allies and partners, and can cut through disinformation when engaging with communities nationally and internationally in crisis events. The globally connected nature of the information ecosystem means that international crises can more easily spark domestic crises – the most recent example being the Israel-Palestine conflict.

To create better national communication strategies, there needs to be greater understanding of the non-English speaking information environment to be effective internationally, and to connect meaningfully with rich cultural diversity in Australia.

Putting together a national information power strategy that includes the non-government sector could be a useful approach. This recognises that much of Australia's information power comes non-government entities, including society itself.

Australia should continue to seize opportunities to work with the private sector to foster a healthy information environment in Australia and to ensure safe and appropriate international communications sales by global companies.

For many participants, holding platforms accountable is the key issue for legislative action. The entire legislative framework around communications probably needs to be reviewed. Laws that were made in the analogue era are no longer fit for purpose. But it is incredibly important that these laws don't silence dissent or inhibit news reporting. This has been seen in the proliferation of strategic lawsuits against public participation (SLAPP) cases which use defamation law to sue individual journalists. SLAPP cases can have a chilling effect on the ability of journalists to hold the powerful and the criminal accountable.

Participants also emphasised the need for Australia to seize this opportunity to work with civil society to strengthen norms around communication. This could include encouraging civil society watchdogs, internet observatories, creating a role for civil society in disinformation legislation, for example, in requiring that platforms need to regularly engage – especially around content moderation.

The transparency of platforms also needs to be addressed. The way in which DIGI has defined transparency needs to be much more specific. There should be requirements about sharing important proprietary information with researchers and regulators as well as individual members of society who request their own data.

Another question is around algorithmic transparency. Should governments have the power to scrutinise the powerful algorithms that decide what content is given preference on social media platforms and search engines?

The risk-based approach to this that the government is taking is probably the right one here, according to one participant. Some algorithms are more harmful than others, so transparency content moderation algorithms are important. As well as some transparency around the training data on LLM AIs. And it would be better to require AI companies to develop quality training data in the first place. And as long as researchers have access to those systems, they can assess the biases and inaccuracies, and develop notions of what a high risk system is, that requires more intervention. And because many of these data bases are offshore, this would require international cooperation.

But to adequately regulate platforms there needs to be a huge upskilling in the bureaucracy, as the government must keep up with this dynamic environment, and to match the resources of tech companies. Regular information literacy training in government is urgent in legal and communications policy areas. Literacy is especially important to members of the armed forces and law enforcement who are a key target of disinformation and radicalisation. NATO has a centre dedicated to this effort – the APS could also develop its own.

WHAT ARE AUSTRALIA'S TOOLS TO SHAPE THE INFORMATION SPACE?

INDUSTRY

- Codes of practice
- Content moderation and monitoring
- Cyber techniques
- Journalism, reporting, analysis and investigation
- Marketing, advertising and PR

GOVERNMENT

- Regulation
- Legislation
- Education and awareness
- Public diplomacy and strategic communications
- Cross jurisdictional cooperation on standards and enforcement
- Consumer protection bodies
- Standard setting, domestic and international
- Ownership of infrastructure and software
- National brand
- National narratives
- State-backed social media accounts
- Institution building

CIVIL SOCIETY AND ACADEMIA

- Community partnerships
- Partnerships with education institutions
- Internet observatories
- Polling and public opinion
- Research and analysis
- Civil society organizations

INDIVIDUALS

- Social media influencers
- Open source investigators
- Patriotic hackers

Barriers

Despite over a decade of increasing disinformation and propaganda, with disastrous consequences for global and national security, many governments in the West, including Australia, have found it difficult to develop a comprehensive and effective strategy to counter to the problem.

There are many possible reasons for this.

Consultees considered that Australian policy makers at all levels have an incomplete grasp of the nature of information environment threats and so have failed so far to act strategically to develop comprehensive legislation to deal with the multiplicity of threats, particularly around the global social media platforms that host the vast majority of disinformation in Australia.

The main enablers for disinformation are major global social media and tech platforms, with powerful and well-funded lobbying capabilities. Their services are now deeply integrated into almost every aspect of government and society. This makes it difficult for a country of Australia's size to influence big commercial players like Google, TikTok, X (formerly Twitter) and Meta. Australia does however have strong alliances and thus an ability to influence standards in cooperation with the US and EU.

Like many countries, Australia has a siloed way of thinking about threats in the information environment, such as cybersecurity, disinformation, social cohesion, foreign interference, data, privacy and criminal exploitation. Agencies do not naturally share information and analysis in a truly integrated way and the best current practice is often to coordinate through interdepartmental taskforces or similar mechanisms. These are usually built around single issue and are non-enduring. Legislation and separation of powers often present barriers to whole-of-government action.

Consultees considered that Australia lacks a mature national consensus on what freedom of speech means in a digital age – that is how a liberal democracy can shape its information environment to ameliorate harm without excessive censorship. National debates often devolve into a binary between "do nothing" or "total control".

There is a perceived deficit in Australia's readiness to influence and shape the information environment actively. It is challenging to raise the level of strategic public communication, especially in a risk-adverse public service. But the cost of not urgently improving this critical function of government creates further information vacuums that will be inevitably filled by disinformation. There is the need to incentivise taking these kinds of risks within government.

Experts consulted said that they struggle to make their insights heard in Canberra policy circles. In the experience of some participants, policymakers often don't take academic researchers seriously. There are not enough forums for experts and policy makers to exchange ideas, so there needs to be a reliable pipeline for this research into the policy world.

The Vision in Practice

What does it look like for Australia to use all tools of statecraft in the information environment?

Australia is enthusiastic about realising its objectives in the information environment as a national priority and takes a leading role in promoting a healthy information space regionally and globally.

It is recognised that, just like the living environment, the information environment requires a definition of what is healthy and the associated caretaking effort to maintain that health. It is not treated as an infinite space to be ignored or left to self-sustain. Australia has a clear and defined vision for what it wants from the information environment from which its national and international efforts flow.

Australia's vision is of itself as an agile, nimble and global actor that can respond quickly and effectively to threats in the information environment. It pro-actively fosters an innovative, resilient and technologically-enhanced information space that supports societal and national interests.

Upholding technological sovereignty in the information environment is a priority, with Australia clearly articulating rights and responsibilities around information and actively promoting them domestically, in the region and internationally, including through resilient information infrastructure. Australia develops a comprehensive and enforceable framework of legislation, grounded in liberal democratic values to constrain harmful actors and encourage good-faith activities in the information environment.

Citizens and governments can easily access a range of trusted sources on any issue, cognisant of issues of legality, privacy and security. Access to digital and other forms of information is available to anyone regardless of personal wealth, cultural background or politics, taking into account the special needs of children and other vulnerable demographics. This information ecosystem supports and is mutually reinforced by learning, innovation, science, facts and accurate discourse.

The information environment enables citizens and governments to connect with their communities in a way that promotes high levels of social trust and political engagement, gives citizens control of personal data and empowers them through education to understand the value of their data. In this way, Australia seeks to further develop the values of the early internet which pointed towards the creation of an online civil society, which was based on values of community, connectivity, inclusion, and accelerated learning.

Australia has an active and ongoing public conversation on the ground rules of free speech in an age of increasingly powerful and intrusive digital technologies. There are clear red lines between the tolerance and acceptance of divergent opinions and the intentional mass distortion of truth. Good-faith, fact-based debate is supported by coordinated networks to counter disinformation.

Australia takes a leading role in supporting credible news at all levels – local, national, regional and global – as a matter of national urgency to counter the tide of disinformation and propaganda that are infecting information systems. There are firm, long-term, well-funded commitments to support an educated, digitally-literate public as sophisticated producers and consumers of information. Media and information literacy should begin at an early age and continue to be accessible as a process of life-long learning about information-related issues and to build individual agency when engaging in the information environment.

To foster a resilient, technologically enhanced information ecosystem at home – one that enables Australians to leverage information to create value while maintaining agency, security, and privacy – Australia should become a world leader in managing standards of conduct by the global information and communications technology sector.

The pursuit of this vision will require a whole-of-nation effort,[20] recognising that much of Australia's information power comes from the non-government cultural, social and economic spheres.

20 AP4D, What does it look like for Australia to take a whole-of-nation approach to international policy (Canberra, 2024), https://asiapacific4d.com/idea/whole-of-nation/

Case Studies

FEDERAL TRADE COMMISSION ANTI-TRUST CASES[21]

Since 2021 the US Federal Trade Commission (FTC) has filed several anti-trust lawsuits against high profile tech companies such as Meta and Amazon. US anti-trust laws had previously focused on the 'consumer welfare standard', with companies generally only targeted over anti-competitive practices if consumers were adversely impacted by increased prices. Under Chair Lina Khan, a scholar and law professor, the FTC has expanded the focus of anti-trust laws and targeted the dominant position of several major tech companies.

EU DIGITAL SERVICES ACT & DIGITAL MARKET ACT[22]

The EU Digital Services Act (DSA) and Digital Markets Act (DMA) aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.

The DSA and DMA have two main goals:

1. To create a safer digital space in which the fundamental rights of all users of digital services are protected
2. To establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally.

The model adopts a legal framework that ensures the safety of users online, establishes governance with the protection of fundamental rights at its forefront, and maintains a fair and open online platform environment.

AUSTRALIAN ELECTORAL COMMISSION

Ahead of the 2022 Federal Election the Australian Electoral Commission (AEC) launched the 'Stop and Consider' campaign,[23] which built on the success of a similar campaign run at the 2019 federal election to help voters cut through misinformation, disinformation and spin. Advertising for the campaign was distributed to voters primarily online via their social media feeds and through digital displays. It was supported by translated material distributed through Culturally and Linguistically Diverse audiences.

The AEC's active and, at times, forthright approach to social media engagement is also a key part of combatting electoral mis and disinformation online. In addition to responding to people who tag the AEC's accounts, the AEC uses keywords to monitor conversations outside of AEC accounts and occasionally jump in to those conversations to provide facts about how electoral processes work.

SWEDISH PSYCHOLOGICAL DEFENCE AGENCY

The Swedish Psychological Defence Agency (SPDA) safeguards Sweden's open and democratic society and the free formation of opinion through identifying, analysing and countering foreign malign information influence, disinformation, and other misleading information directed at Sweden or at Swedish interests.[24] The main mission of the SPDA is to lead the coordination and development of Sweden's psychological defence in collaboration with public authorities and other stakeholders in society. SPDA offers support to government agencies, municipalities, regions, the business sector, and organisations, as well as contribute to strengthening the resilience of Sweden's population:

"A strong psychological defence is not just a matter for the Swedish Psychological Defence Agency, it requires a whole of society approach where agencies, municipalities, organizations and not least – the individual citizens work together."

21 https://www.theguardian.com/technology/2023/sep/27/ftc-head-lina-khans-fight-against-amazon-has-been-years-in-the-making
22 https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
23 https://www.aec.gov.au/media/2022/04-12.htm
24 https://www.mpf.se/en/

DEBUNKING HANDBOOK 2020[25]

The Debunking Handbook is a free resource written by leading experts that describes the best ways to combat misinformation. Building on an earlier 2011 version, the 2020 Handbook is a consensus document that was created by an innovative process that involved a series of predefined steps, all of which were followed and documented and are publicly available. The Handbook unpacks the science of debunking for engaged citizens, policy makers, journalists and other professionals. It distils the most important research findings and current expert advice about debunking misinformation.

BEYOND FAKE NEWS[26]

In November 2018 the British Broadcasting Corporation (BBC) launched Beyond Fake News – an international anti-disinformation initiative. The project aims to fight back against disinformation with a major focus on global media literacy, panel debates in India and Kenya, hackathons exploring tech solutions and a special season of programming across the BBC's networks in Africa, India, Asia Pacific, Europe, and the Americas. As well as reporting, the Beyond Fake News website contains education and training resources that encourage people to think critically about what they read, see and view so that they can spot misleading or bad information and resist sharing content that might be false or out of context.

EUROPEAN DIGITAL MEDIA OBSERVATORY[27]

The European Digital Media Observatory (EDMO) is a project that supports the independent community working to combat disinformation. It serves as a hub for fact-checkers, academics and other relevant stakeholders to collaborate with each other, while encouraging them to actively link with media organisations, media literacy experts and provide support to policy makers. The creation of the Observatory is one of the elements in the European Commission's detailed action plan against disinformation.

The activities of EDMO are based on 5 strands:

1. mapping fact-checking organisations in Europe and supporting them by fostering joint and cross-border activities and dedicated training modules.
2. mapping, supporting and coordinating research activities on disinformation at European level, including the creation and regular update of a global repository of peer-reviewed scientific articles on disinformation.
3. building a public portal providing media practitioners, teachers and citizens with information and materials aimed at increasing awareness, building resilience to online disinformation and supporting media literacy campaigns.
4. design of a framework to ensure secure and privacy-protected access to platforms' data for academic researchers working to better understand disinformation.
5. support to public authorities in the monitoring of the policies put in place by online platforms to limit the spread and the impact of disinformation.

25 https://skepticalscience.com/debunking-handbook-2020-downloads-translations.html
26 https://www.bbc.co.uk/beyondfakenews/
27 https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

PACIFIC MEDIA ASSISTANCE SCHEME[28]

The Pacific Media Assistance Scheme (PACMAS) is a long-term media development program that works to support Pacific media's role to hold space for locally led civic discussion and debate. PACMAS delivers capacity building activities that support credible news journalism, digital transformation, quality content production and media association strengthening.

The initiative is an Australian development assistance project, funded by Australia's Department of Foreign Affairs and Trade (DFAT) and managed by ABC International Development, which works in partnership with the Pacific Islands News Association, national media associations and Pacific media businesses.

AUSTRALIAN MEDIA LITERACY ALLIANCE[29]

The Australian Media Literacy Alliance (AMLA) is an unincorporated group of organisations whose objectives in the area of media literacy are closely aligned.

AMLA's efforts focus on supporting lifelong learning especially for those who may be vulnerable to disinformation or digital exclusion. Through consultation, research and advocacy, AMLA's primary goal is to develop and promote a government-endorsed national media literacy strategy for Australia, which will:

- State the importance of media literacy for all in society
- Articulate the achievements and challenges in the Australian context
- Provide direction for educators and curriculum development
- Raise awareness and encourage a whole-of-community response.

LATERAL READING EDUCATION[30]

A project funded by the ACT Education Directorate – UC Affiliated Schools Research program and the US Embassy in Canberra teaches students in Years 4, 5, and 6 from four ACT schools to 'think like a fact-checker' by employing a Civic Online Reasoning framework.

In practical terms, this means that students should not engage 'vertically', either by scrolling down the page, or by analysing a claim in depth. Instead, students should learn about a source of information by leaving the webpage, opening another tab on a browser, and searching elsewhere: a concept known as 'lateral reading'. If the claim or source is found to be reliable, students can investigate in more depth, but if it is not, they should move on

In an earlier project, an assessment of online reasoning was administered to students six weeks prior to the intervention and again five weeks after. The results indicated that students in the treatment group were significantly more likely than students in the control group to have shown gains from pre-test to post-test.[31]

28 https://www.abc.net.au/abc-international-development/pacmas-about/102240758

29 https://medialiteracy.org.au/

30 Mathieu O'Neil, Robert Ackland and Rachel Cunneen, Building resilience with information literacy and information health, August 2023, p. 19, https://apo.org.au/sites/default/files/resource-files/2023-08/apo-nid323760.pdf

31 Sam Wineburg, Sarah McGrew, Joel Breakstone and Teresa Ortega, Evaluating Information: The cornerstone of Civic Online Reasoning. Stanford History Education Group, 2016, https://purl.stanford.edu/fv751yt5934

Pathways

Australia has already undertaken a range of measures to manage the information environment, detailed above.

These efforts are welcome steps and Australia has often been a first mover in this space – as, for example, with negotiating with online platforms to pay for news.

But these measures have not been enough to stem the tide of disinformation in both the national and global information environment.

The experts who contributed to this paper offer the following recommendations as a contribution to realising a positive vision of a healthy, safe, engaging and democratic information ecosystem.

A NATIONAL BODY FOR THE INFORMATION ENVIRONMENT

Australia should create a national body that identifies and pre-empts emerging problems in the information environment and marshals resources and expertise to find solutions. This body would draw together, and coordinate work being done in individual agencies across government and include mechanisms to engage in dialogue with, and draw on the expertise of, non-government actors such as industry, civil society, non-governmental organisations and academics working in the space. This requires a legislative basis.

Such a body would help government create a strong, enforceable regulatory framework that sets a standard of conduct, as well as legal parameters for foreign technology companies operating in Australia. It should function as a vehicle that promotes constant dialogue between government, industry and the Australian public.

Consultees had a range of views on the role of government in the information environment. Some argued that the government should keep its role as minimal as possible by setting the conditions for a healthy information ecosystem and keeping direct intervention to a minimum. This would include providing economic incentives and nudging but would be wary of being too restrictive. One participant pointed to the current disinformation legislation before Commonwealth Parliament and the danger of giving the government of the day too much power to define what is and is not disinformation and suggested that the approach should be incentivising platforms to create an information environment that better serves the public interest.

However, others argued that a low-key role for government may prove ineffective given the constantly evolving threats in the information domain.

Participants agreed that one of the most important things that all branches of government can do is set high standards of truth and to develop the facility for strategic pre-bunking and rapid response help prevent disinformation from becoming normalised in Australia's political system.

It may also be useful to create teams in government departments with one dissemination point that are responsible for calling out coordinated disinformation that targets Australia as soon as it appears and demonstrating to the public and disinformation networks that the government is aware and responding. This could be especially valuable in a time of national or regional crisis. One model could be the Department of Foreign Affairs and Trade's Smartraveller program.[32]

INCREASE RESOURCING FOR PROFESSIONAL STANDARDS BODIES IN THE INFORMATION ENVIRONMENT

The ability of standard setting and accountability bodies such as the Australian Communications and Media Authority to undertake oversight and hold those who breach standards to account is currently limited by resource constraints. The government should increase resourcing for bodies that oversee professional standards in the information environment in line with the impact that this space has across all aspects of Australian society. This should include re-focusing scrutiny on 'traditional' media, as well as developing and updating guidelines for emerging technologies such as generative AI.

32 Department of Foreign Affairs and Trade, "Smartraveller", https://www.smartraveller.gov.au/

Investment in domestic standards bodies would also better equip Australia to contribute to and influence the development of global norms around standards.

STRENGTHEN REGULATION AND OVERSIGHT OF SOCIAL MEDIA PLATFORMS

The government should also strengthen regulation over key elements of the business model of major social media and other information- and data-gathering platforms, such as third-party data-brokering, targeted advertising and recommendation algorithms.

In the case of anti-disinformation legislation, some consultees recommended that the government not set a threshold definition for disinformation, but instead provide for an inclusive, dynamic, democratic process of negotiating what is and isn't acceptable in the information environment.

Part of this effort needs to be the co-design of a binding framework (at minimum a memorandum of understanding, and ideally a mandatory code of practice) around content moderation on social media platforms that involves the participation of civil society, government, media, researchers and industry. This could look like a more inclusive version of the Facebook Oversight Board and would also include negotiating better access to social media content for disinformation researchers.

Current regulation relating to child exploitation material, or the livestreaming of terrorist attacks offer a useful precedent of social media entities collaborating with government to prevent the propagation of harmful material. This could provide a model for combating information operations which, from an operational viewpoint, have signatures that are different from typical social media behaviour.

There also needs to be an urgent consideration of what regulation needs to look like as generative artificial intelligence (AI) begins to flood the internet. To this end, Australia needs to immediately find ways to work with companies like Open AI, to ensure that new AI products are transparent, safe, and will not cause the further breakdown of the information environment.

STRENGTHEN TRANSPARENCY, INVESTIGATION AND ENFORCEMENT FUNCTIONS

Given the complexity of the technology involved as well as the size and power of tech companies, the government should ensure that it has the power and the data – and sufficient resources – to properly investigate breaches of legislation such as the 2022 Optus and Medibank privacy breaches.[33] It needs to be able to act quickly and decisively, which means a strategic and pre-emptive approach to monitoring disinformation networks online.

SUPPORT AUSTRALIAN DIASPORAS TARGETED BY DISINFORMATION AND HARASSMENT CAMPAIGNS

As an adjunct to a national, strategically focused body, Australian intelligence and security organisations should also work more closely with other government bodies to strengthen the capacity to provide tangible and rapid support to Australian citizens targeted by malicious foreign actors. As a first step, the government should undertake a multilingual campaign to raise awareness of the national security hotline among members of the public who may not be aware of it.

One consultee gave the example of Australian citizens targeted online by the Iranian regime. Interference in Australia's Chinese, Russian, Ukrainian, Rwandan, Sudanese communities has been well-documented and is likely to keep increasing. This targeting can include repeated and persistent online threats of physical violence to individuals and their families, false accusations of criminal activity, persistent dehumanising language and the hacking of citizens' computers.

33 Josh Taylor, "Australians increasingly concerned about online privacy after high-profile cybersecurity breaches", The Guardian, 8 August 2023, https://www.theguardian.com/australia-news/2023/aug/08/australia-cybersecurity-laws-hacks-optus-medibank-privacy-data-breach

In addition to increased information sharing and collaboration between security and intelligence organisations and other government agencies, a rapid response capability could be achieved by further expanding the remit of, and a concomitant increase in resourcing for, the eSafety Commissioner to support diaspora groups being targeted. As the most public-facing Australian body for safety from online crime and exploitation, embedding such a mandate within the eSafety Commissioner is an option that is less likely to trigger political sensitivities.

DEVELOP A COMPREHENSIVE PUBLIC LITERACY AND INFORMATION CAMPAIGN

The government should develop a long-term public communications strategy that actively supports truth-based communication and that consistently makes the case for science, for facts and for accurate information. Consultees stressed that the content of these campaigns need to be extremely engaging, using the best Australian creative talent, to cut through and needs to be aimed at multiple Australian audiences across all media platforms.

A key feature of this would be a comprehensive digital media literacy campaign that clearly articulates:

- values of press freedom, media ethics, privacy and freedom of speech
- what constitutes hate speech, on-line bullying and trolling, disinformation and propaganda
- the critical thinking skills needed to be resilient in the face of cognitive manipulation and exploitation
- how to navigate the internet as synthetic, manipulated images and text created by generative AI become widespread

The program should be well-funded, long term and take place from primary education level onwards. The content should be fun and engaging, with face-to-face learning and collective problem solving emphasised. This would need to include support for educators and teachers to help them combat disinformation in the classroom.

Regular broad-based public information campaigns on recognising disinformation and propaganda using engaging creative content are equally important.

These campaigns need to be ramped up around elections to ensure a minimum of manipulation. However, there is a question mark over whether public literacy campaigns would work in the case of generative artificial intelligence (AI). As the technology improves, most research shows that when people are asked to distinguish between a digitally manipulated or fake image and a real one, they will almost always choose the fake image.

In addition to broad based public awareness campaigns, digital media literary needs to be included in education curriculums from early childhood onwards, to help children and young adults build resilience against the many harms targeted at them in the information environment.

In thinking about such a framework, radicalisation prevention and support strategies should be built into education programs that deal with the information environment. Young adults, especially young men, are prime targets for radicalisation. Consultees suggested that elements of a successful education campaign would include: learning how to recognise disinformation and propaganda aimed at radicalisation, the individual vulnerabilities that radical groups use to exploit and recruit, the harmful and violent nature of radical groups and their financial and political aims, a clear demonstrations of the real world consequences of online violence, and easily accessible off-ramps for individuals who have already been radicalised but want to escape these groups.

These off-ramps could include grant funding for civil society de-radicalisation groups that run online chat groups to support those trapped in radical groups, requiring social media companies to de-amplify radical content and algorithmically promote de-radicalisation support groups, and building a community of practice among psychological health practitioners specialising in re-radicalisation.

Much more support is needed for survivors of online hate and special consideration needs to be given to women – as misogyny and violence against women is the through-line that connects all radical online ideologies. Researchers who have contributed this report warn that

hatred against women is becoming more widespread and normalised in online culture, noting the potential of social media for mass radicalisation rather than just radicalisation of fringe individuals. These researchers recommend strong legal measures, such as criminalising online sexual violence such as deep fake pornography in a similar way to real world sexual harassment and assault.

SUPPORT CIVIL SOCIETY ORGANISATIONS ADVOCATING FOR DIGITAL RIGHTS

Many human rights champions have noted that a strong civil society is critical to safeguarding rights. Even democratic governments sometimes have strong incentives to trade rights away, to use the power they have to entrench their own power by targeting critics and removing alternatives.

The Australian Human Rights Commission could lead an effort to promote more civil society organisations working to further digital rights. A human rights bill in Australia could provide a stronger legal anchor to these efforts. In addition, the government could earmark funds to support to civil society human rights organisations at all levels – as well as to civil society more broadly as part of a civil defence against anti-democratic forces, including those that manifest in online environments.

At this current moment, human rights organisations are too under-resourced to grapple meaningfully with the issue of digital rights. For example, groups in the National Women's Alliance often have two or three staff, and there no high-profile organisations focused on how to protect the basic human rights of women online.

There also need to be mechanisms created to connect researchers with civil society advocates and problem solvers on this issue, and policy makers would be well served by better, comprehensive and consistent research on public attitudes towards social media and online life.

Another thing to be considered is measures to improve access to justice for online harms, which could include creating a legal defence fund that can be accessed by vulnerable groups to pursue online abusers.

And there also needs to be funding available for civil society organisations to invest in cybersecurity. Globally and in Australia, these organisations are subject to cyberattacks, hacking and denial of service (DoS) attacks, mostly from hostile authoritarian governments but also from powerful actors within democratic nations.[34] The same applies to news organisations, where especially smaller, investigative organisations are being targeted by increasingly confident authoritarian forces.

SUPPORT FACT-CHECKING ORGANISATIONS

Part of this public literacy strategy could include providing adequate and long-term funding to non-partisan fact-checking authorities operating at arm's length from government. This would help elevate the work of fact-checkers in public debates and would demonstrate a commitment to transparency and accuracy.

It should be noted that existing fact-checking bodies – most often located in universities – need urgent support.[35] They are often resource-poor at the same time as coming under constant attack from powerful partisan forces who may be keen to see a politics of disinformation take hold. The more credible fact-checkers there are in an information system, the harder it is to attack the notion of fact-checking.

It is critically important that fact-checkers are able to scrutinise political claims. One sign that a political culture of disinformation is developing is when elected political officials regularly make easily disprovable false claims with seeming impunity because they are backed by a partisan media ecosystem. In theory, these claims may be easily disproven, but in an information environment eroded by disinformation, emotive false claims are powerful. When those with strong professional norms around truth-telling and verifiability have already been systematically attacked – such as fact-checkers, academics, journalists and public servants – it will be much harder for their fact-checking to gain traction.

A legislative approach to disinformation could require social media platforms to fund fact-checkers in the countries in which they operate, or to have contributor moderation policies like X's Community Notes.

New generative artificial intelligence (AI) technologies also need to be urgently explored for their fact-checking potential, keeping in mind that these technologies currently have a problem with accuracy, verifiability and bias. Generative AI has the potential to completely overwhelm the resources of factcheckers, both within and outside newsrooms, as well as the attention of the public in trying to keep up with verifying misleading images. This is a huge challenge which needs gatekeepers at every level of AI image, text and sound generation.

There also needs be more media space given to entities that can broadcast what is true consistently rather than waiting on events to report on something. Wikipedia serves this function but is vulnerable to coordinated disinformation attacks, DoS attacks, government censorship, a dwindling number of editors and declining levels of fundraising from readers. It also privileges text-based information.

FOCUS ON PRE-BUNKING DISINFORMATION

Australia needs to find a systematic way for government and media to pre-bunk – or pre-emptively debunk – likely areas of disinformation. Many studies have shown that pre-bunking is an effective tool in countering false information. It may also be more scalable than retrospective targeted debunking.

At the government level, a much-cited example of this was the US declassification and release of intelligence showing Russia's intention to invade Ukraine, which to some degree frustrated Moscow's attempt to set the narrative around the invasion.[36]

This effort would require a change of culture in government communications teams, which are currently extremely reactive. They would need to hire disinformation specialists and have access to information on disinformation narrative trends.

It is important to note that pre-bunking of visual disinformation in the form of memes and deep fakes is critical here, as is being able to predict the kinds of disinformation narratives that will emerge out of events so as to pre-emptively seed truthful framing of these events.

SUPPORT A STRONG, DIVERSE PUBLIC INTEREST JOURNALISM SECTOR

Public interest journalism – journalism that supports accountability in a democratic society – has been in jeopardy ever since the advertising model that sustained it migrated to social media. Google and Meta now between them account for 80% of the online advertising market.

Since public interest journalism can no longer depend on advertising or online subscriptions for long-term survival, in both metropolitan and regional areas, the government should urgently support measures to develop large-scale alternative sources of funding.

If current trends continue without intervention, the result will probably be the further concentration of news organisations into ever tighter global monopolies, with national and regional news resources collapsing.

The Australian government has already attempted to support news income through the 2021 News Media Bargaining Code, whose purpose was to make large

34 Shannon Bond, "Elon Musk sues disinformation researchers, claiming they are driving away advertisers", NPR, August 2023, https://www.npr.org/2023/08/01/1191318468/elon-musk-sues-disinformation-researchers-claiming-they-are-driving-away-adverti

35 RMIT FactLab, "Funding", https://www.rmit.edu.au/about/schools-colleges/media-and-communication/industry/factlab/about-rmit-factlab/funding

36 Julian Barnes and Adam Entous, "How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans", New York Times, February 2023, https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html#:~:text=Biden%20agreed%20and%20directed%20that,a%20broad%20group%20of%20allies.&text=%E2%80%9CHe%20turned%20to%20us%20in,in%20a%20speech%20last%20week.

social media platforms operating in Australia pay for news content. However, with the likely demise of this agreement, announced by Meta this year, it is time to consider other measures such as a special digital platform tax, the revenues of which could be channelled towards news.

And given Meta has also signalled that it will no longer promote news and political content on its sites, an additional requirement could stipulate that platforms are required to promote credible and accurate news content.

In addition, the government needs to support Australian news organisations in their consultations with AI companies, as these companies attempt to integrate live news into chatbots and other AI products. Smaller news players especially need support.

To encourage diversity, this support for news journalism must be done in a way that does not entrench existing news organisations and information monopolies but encourages new players to emerge.

Complementary policies could include tax incentives for news producers as well as for philanthropic support. Not-for-profit or employee-owned corporate structures for media companies could be modelled and encouraged. The most well-known of these is the Scott Trust which owns The Guardian. These kinds of trusts could be replicated in Australia to provide stable base funding and freedom from political interference.

Another approach could tackle the demand side in the form of government funding for news subscriptions that are distributed on the basis of means testing. Given that most credible news is now only accessible through prohibitive pay walls, restoring public access to diverse and accurate news sources has become a critical issue.

It may also be useful to find ways of supporting the de-commercialisation of some aspects of the digital public square so that it is able to support an accurate public information commons. Wikipedia is an example of a successful non-commercial model.

Secure, long-term funding should also be given to establish public disinformation research teams and internet observatories in universities.

A public interest non-partisan think tank devoted to aggregating this research and promoting national public debate on issues on the intersection of information, democracy and national security should also be funded. A model worth considering here is something like the European Digital Media Observatory, which could be funded through disinformation legislation. It would be multidisciplinary and produce reports and media content, acting as a kind of expert civil society watchdog for platforms operating in Australia.

These measures could be accompanied by a broad-based multiplatform media product which aggregates the disinformation research being done in Australia and overseas as a resource for government, researchers and the public. Such a product could be hosted by existing public interest media organisations, such as The Conversation, which may be more trusted than a directly funded government channel.

USE INTERNATIONAL DIPLOMACY FOR A HEALTHY GLOBAL INFORMATION ENVIRONMENT

Tackling the structural issues involved in the increasing spread of disinformation and propaganda will not be possible without developing greater strategic alignment with allies and partners in working for a healthy global information environment. This will require commitment of resources to create mechanisms for consistent, regular and results-based international engagement on this issue. This would entail a clear recognition that the same forces that are spreading disinformation online are also attacking the multilateral system that is grounded in ideas about the rule of law and universal human rights.

For example, Australia might want to explore a more unified approach to disinformation and platform regulation with the US and EU, to better address the cross-jurisdictional nature of the disinformation problem. This might include coordinated support and further development of norms that embed access to accurate information as a human right. It may be building communication networks to deal with global public health crises stemming from conflict, pandemics and climate change.

Another measure could be to exchange research, policy ideas and intelligence on disinformation and to protect researchers from being targeted by disinformation networks and the political actors that use them. A unified approach might also mean partnering to support a body like the Facebook Oversight Board, but with a broadened remit to include multiple platforms. This body would incorporate strong community feedback mechanisms and would require platforms to have robust complaint and feedback processes.

Another area for consideration is working with partners and allies on the application of legal and financial sanctions against enablers of disinformation, online exploitation and human rights abuses. As one example of these kinds of measures, the EU will has put forward financial sanctions of up to 10 percent of global revenue against digital and broadcast media companies that ignore EU directives for the removal of disinformation networks from their platforms. In another example, the US Department of Commerce has recently blacklisted a Canadian company Sandvine for providing online censorship and surveillance tools to the Egyptian government which were used to block news and to target political actors and human rights activists. Australia could consider supporting these efforts through similarly aligned sanctions measures, perhaps through the Magnitsky Act.

INCLUDE DISINFORMATION IN ELECTION AND GOVERNANCE SUPPORT

2024 will be a watershed election year, with 60 elections affecting 4 billion people. All these elections will struggle with disinformation. When Australia supports free and fair elections though UN processes and other multi- and bilateral relationships, it could also develop a system of support to help countries deal with disinformation through election cycles. Seeing promoting a truth-based information environment as part of Australia's development partnerships – including making this a centrepiece of Australia's brand abroad – could boost the nation's influence in the region and in its relationship with allies.

SUPPORT RESILIENT INFORMATION INFRASTRUCTURE

Where access to information infrastructure is an issue – due to geography, lack of electricity, poor distribution of print media or digital access being cut due to a natural disaster – Australia and partners will need to think more creatively about developing alternative information pathways. For example, when an earthquake in Tonga damaged its undersea cable, the island was cut off from information flows. Starlink was able to reconfigure its constellation in Tonga's direction to restore some information flows which was critical in dealing with the disaster.

These actions could also contribute Australia's strategic communications capability by identifying the kinds of information assets that Australia might need to deploy in both friendly and hostile conditions. For example, in a humanitarian and disaster relief (HADR) effort, Australia might need to communicate directly to reach people on the ground.

INCREASE INVESTMENT IN INDO-PACIFIC MEDIA

Consultees recommended that Australia's strategy for regional outreach should be urgently expanded to match the magnitude of the information environment challenges in the region. This includes supporting regional broadcasting and news, regional cultural content and storytelling, a social media strategy to promote credible information, and disinformation literacy training. Non-government entities should be involved in all these efforts.

It should be noted however that outreach to the region on bolstering credible, accurate journalism and countering propaganda and disinformation will face a number of cultural and political challenges. These include cultural and language barriers, lack of understanding of regional social media, regulatory and disinformation ecosystems, illiberal political and cultural environments in which ruling elites have embraced both media censorship and the disinformation as tools of political rule, as well as of foreign and security policy.

Australia is already active in this space, mostly in the Pacific. Consultees praised the Pacific Media Assistance Scheme, which is supporting several independent media reporting projects. While the quality of the program is good, it is not operating at the scale needed to achieve the objectives of preserving a free, open, diverse and credible media in the region.

For example, Australia's Pacific broadcasting strategy still spends less than one Australian dollar per capita compared to Japan which spends roughly $4.50 on overseas broadcasting and Germany which spends $7.00 per person. Research from the Lowy Institute shows that over decades there has been a policy gap on strategic communications that underestimates the role of the media in enhancing Australia's soft power and leveraging it to achieve its objectives internationally.[37] This blind spot must be urgently addressed to navigate this era of fast spreading disinformation.

A quadrupling of the regional broadcasting budget – approximately 0.6 of the development budget – would a be a useful benchmark, according to some participants. Funding that is currently going to public relations could be redirected into supporting independent media regionally.

In doing this, Australia would need to have a very transparent agenda in supporting independent verified information, one which would include submitting Australian policy and action in the region to scrutiny.

Participants reported that the outlook for independent media in the Pacific is dire. Pacific media needs support in the form of training and resources to transition to digital, and to deal with disinformation, including highly manipulated images.

Support for management is also critical in three major respects. One is training managers in up-to-date management methods that encourage young journalists, especially women, to stay in the sector. This training would cover issues like respect at work, flexible working hours and zero tolerance for bullying and sexual harassment.

The second issue is finding sustainable digital business models that can support public interest journalism. This could include looking at charitable trusts, non-profit and collective ownership models.

A third issue faced by regional media managers is in creating a reliable pipeline of media talent. It was noted that many young journalists in the region are being invited to China to undergo media training and come back with Chinese talking points, publishing Chinese press releases.

Australia should invest in substantive journalism training – not just for a few weeks, but ongoing – to support a culture of accurate, credible and accountable journalism and analysis. Australia could also invest more in supporting the wages of journalists through its development program. Small media organisations looking for a financial lifeline are vulnerable to capture by foreign and domestic elements interested in subverting press freedom, so this is an area where Australia could make a big difference for a small cost.

Another element is strengthening the professional networks of reporters, presenters, producers and editors in the region. Threats to media freedom are rising from foreign and domestic forces. Media organisations are doing their best to help their members push back against these pressures, but these organisations have few resources and are often run on a volunteer basis. Providing funding for one or two paid staff members would help make these organisations more effective. Consultees mentioned that in countries such as Papua New Guinea, the media is facing restrictive legislation. The media needs to be able to be strong stakeholders and to act before press freedoms are legislated out of existence.

Similarly, networks outside the region can be extremely valuable. For example, public sector media in Australia will report on the region when commercial media fails to do so for financial reasons. As a result, Pacific journalists sometimes leak to trusted Australian journalists to get an important story covered. But public broadcast media would need to fund at least one permanent Pacific correspondent, based in nations like Fiji and Vanuatu for this dynamic to become more effective.

37 Annmaree O'Keeffe and Chris Greene, "International Public Broadcasting: A Missed Opportunity For Projecting Australia's Soft Power", Lowy Institute, December 2019, https://www.lowyinstitute.org/publications/international-public-broadcasting-missed-opportunity-projecting-australia-s-soft-power

Restoring news and public interest media in the region is critical to countering a rising tide of disinformation. With Facebook dominant and newspaper sales falling, quality mainstream media has an important role. This was especially evident in Fiji during the COVID-19 pandemic, where the community was dealing significant mis- and dis-information. The Fiji Times had an hour-long live program which dealt with false information about the pandemic, hosting local doctors on air. This approach was very influential in maintaining public health and social stability during the crisis.[38]

Consultees considered that disinformation flows in the region come mainly from China, North America and Indonesia. Most recently, journalists have noted rising levels of propaganda and disinformation from Israel, which finds fertile ground in a heavily religious region that considers the nation to be the biblical Lost Tribe. There are propaganda and disinformation campaigns coming out of Jakarta are aimed at eroding support for West Papuan independence.

If nothing is done, consultees warned, in a decade there will be no credible news left in the region. Even now, once reputable sites in PNG are now publishing graphic torture images and are flooded with non-critical stories about sorcery. As these stories have been widely disseminated by social media, belief in sorcery – which used to be confined to the Highlands – has now taken hold in coastal areas.

The creation of disinformation observatories would be extremely useful here. These could consist of a Facebook page run by two or three journalists that track and call out disinformation narratives across the region. One example of this low-cost approach in the area of news aggregation is the Pacific Newsroom Facebook page, which consultees agreed was an invaluable resource, aggregating the region's best independent news. It is currently run by volunteers. This model could also be applied to a disinformation resource, but it is important to note that volunteer models are probably not sustainable in the long term and would need funding support.

For even more effectiveness, Australia needs to explore the potential to work with the United States on media in the Pacific. Australia has been leading on media development in the region on a shoestring budget, however USAID has just announced a program to support media in the region which in budgetary terms dwarfs what Australia has been able to do.

Australia could also help the Pacific to negotiate with major social media platforms to remove harmful coordinated disinformation networks and to navigate cultural nuances: for example, posts of Pacific people painted for ceremonies are often taken down because they contain nudity.

Beyond news, Australia could partner with Pacific talent to create cultural storytelling content, comedy and drama series, talk shows, podcasts and a variety of other content forms, showcasing Pacific culture.

All these actions would help build trusted, non-transactional relationships in the region and preserve the flow of factual information. Without good reporting, it is very difficult to formulate defence, development and diplomatic strategy and to verify intelligence – in essence to get any kind of accurate picture of a region so important to Australia's interests.

38 The Fiji Times, "COVID-19: FNU to host seventh series of 'Explain the Science' today", June 2021, https://www.fijitimes.com.fj/covid-19-fnu-to-host-seventh-series-of-explain-the-science-today/

Contributors

Thank you to those who have contributed their thoughts during the development of this paper.

Views expressed cannot be attributed to any individuals or organisations involved in the consultation process.

Aaron Kearney OAM
ABC International Development

Alice Dawkins
Reset.Tech Australia

Alice Ridge
International Women's Development Agency

Andrew Erbs
Catalpa

Anne-Louise Brown
Cyber Security Cooperative Research Centre

Bella Anis
Juta Mewangi Enterprise

Ben Bohane
Australia Pacific Security College

Chris Mesiku
ANU School of Cybernetics

Chris Zappone
The Age

Claudine Ryan
ABC International

Dara Conduit
University of Melbourne

Eryn Newman
ANU School of Medicine and Psychology

Geoff Heriot
Independent consultant and author

Glen Edwards
Elysium EPL

James Holden
Duolingo

Jemima Garrett
Australia Asia Pacific Media Initiative

Josh Copland
CMAX Advisory

Lucy Albiston
Australian Strategic Policy Institute

Mary-Louise O'Callaghan
Médecins Sans Frontières Australia & New Zealand

Mathieu O'Neil
University of Canberra

Matthew Griffin
Independent Consultant and Researcher

Michael Davis
UTS Centre for Media Transition

Michael Barnes
ANU Machine Intelligence & Normative Theory Lab

Michael Jensen
University of Canberra Institute for Governance and Policy Analysis

Oliver Stelling
Future Score Communications

Sue Ahearn
The Pacific Newsroom

Shannon Zimmerman
Deakin University

Sharon Cowden
Former Australian Federal Police

Spiro Polycandriotis van Duynhoven
Former diplomat

Sushi Das
RMIT FactLab

Tanya Notley
Western Sydney University Institute for Culture and Society

William Stoltz
ANU National Security College

AP4D thanks the Australia Asia Pacific Media Initiative for arranging a consultation session to assist the development of this paper.

EDITORS

Anastasia Kapetas
Advisor

Tom Barber
Program Manager

Melissa Conley Tyler
Executive Director

AP4D
Asia-Pacific Development, Diplomacy & Defence Dialogue

FOUNDING PARTNERS AND SUPPORTERS

Australian Council For International Development

The Institute for Regional Security

IDCC

Australian National University

The University of Melbourne