Department of Infrastructure, Transport, Regional Development, Communications and the Arts

information.integrity@infrastructure.gov.au

Phone: 1800 075 001

GPO Box 594
Canberra ACT 2601

To whom it may concern,

We are writing to make a submission to the exposure draft of the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023*. The Australian Citizens Party (ACP) adamantly opposes this law, which is a dangerous vehicle of censorship and discrimination.

The ACP, as a firm proponent of Australia's economic and political sovereignty, a staunch anti-war advocate, and critic of political corruption, consistently publishes content which is opposed to mainstream media narratives and the views of the government of the day. The ACP has already been targeted for censorship if the proposed laws are introduced, which we have detailed in our submission.

Please find attached our submission, including two case studies which illustrate our concerns over the proposed law, and additional research in support of our views.

Yours sincerely,

Melissa Harrison	Robert Barwick
Researcher	Research Director

1. ACMA Bill will have Orwellian consequences

The proposed *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023* provides the Australian Communications and Media Authority (ACMA), "with new powers to combat online misinformation and disinformation". The Australian Citizens Party (ACP) believes that this law is another dangerous lurch down the path to totalitarianism which all Australians should oppose. The Bill gives the government power to regulate "truth" online by being able to force social media platforms to censor "misinformation" and "disinformation" that is "harmful"— three vague terms that are open to very broad interpretation.[1]

On the 120th birthday of George Orwell, author of the book Nineteen Eighty-four, in which a totalitarian government regulated the truth, the Australian Government announced that it would introduce legislation which heads down that path, here in Australia. The Bill excludes content which is authorised by either federal, state or local governments from being deemed "misinformation". In other words, anything authorised by Government cannot be held to be misleading. One only has to consider the Government position on the Iraq invasion, or during the COVID period or the background behind what is presently occurring in Ukraine—the government position cannot be classed as "misleading", unlike any position which opposes that Government line.

If ACMA determines some content to be "misinformation" or "disinformation" it can at its option issue potentially huge penalties, which would quickly cause most companies or individuals to comply and exclude or remove the complained-of content or go out of business. There is no limitation in the Bill of what "standards" might be imposed by ACMA if it decided to issue a standard applying to particular social media providers rather than endorse a voluntary code.

It is difficult to see how this legislation in its present form could be simply amended to make it workable without incorporating unacceptable risks of the Nineteen Eighty-four-type consequences. It should not be administered by an unaccountable body but administration by the current political class would be of comparable concern. If there is to be any limitation on content, it should be clearly and unambiguously defined. There are many obvious examples, we can all think of things that should not be broadcast, but it is difficult to define them in some general way. There should not be any definition which incorporates an ability to determine what is "truth".

The fact that the bill explicitly exempts any government communication, of any level of government, from being considered misinformation or disinformation, shows how Orwellian this law will be. While the bill's penalties won't apply to individuals, it will enforce a regime of suppression of any speech on social media that undermines government claims. It would not just apply to protecting public health, as we have already witnessed in the mass-censorship of contrary analysis relating to COVID-19, including of qualified doctors and scientists. It would also apply to debates on foreign policy, such as whether Russia or China are "threats" to Australia, which the government claims to justify committing almost $1 billion to arming NATO's proxy Ukraine against Russia, or promising $368 billion to buy US and British submarines to deploy against China.

[1] See the ACP's attached legal analysis of the proposed Bill, 'Documentation: the ACMA social media censorship bill and its Orwellian implications'

2. ACMA's judgement already dubious

The government has described the new proposed powers for ACMA as being "consistent with the key recommendations in the ACMA's June 2021 Report to government on the adequacy of digital platforms' disinformation and news quality measures". However, ACMA's report itself contained examples of the regulator's dubious judgement in determining what is misinformation. This raises serious questions over the wisdom of allowing ACMA, or any such organisation, to be an arbiter of truth.

For example, ACMA's June 2021 report included a lengthy case study on "false, misleading or unproven narratives arising from the COVID-19 pandemic", which aimed to provide insights into "the range, spread and impact of disinformation and misinformation in Australia, providing a baseline to inform future thinking and developments across government and industry."

ACMA examined what it determined were four "distinct online misinformation narratives", which were "anti-vaccine, anti-5G, anti-lockdown and QAnon". If at this time of this report, ACMA had possessed powers proposed in this Bill, online discourse concerning these so-called "misinformation narratives" could be censored at ACMA's direction. However, there are serious questions over ACMA's judgement. For example, "anti-lockdown" views, which ACMA determined were "misinformation", would certainly have been expressed by some of the 3,000 public housing residents of North Melbourne who were abruptly forced into a hard lockdown and banned from leaving their homes in early July 2020.[2] Many of the vulnerable residents reported that they did not receive adequate food supplies—would their pleas for help or complaints over their treatment be considered "anti-lockdown" "misinformation" by ACMA?

Similarly, ACMA deemed "anti-vaccination" views as "misinformation narratives". However, around six months after ACMA's June 2021 report was published, the Australian government established a Covid-19 vaccine injury claims scheme, to which thousands of Australians have submitted claims.[3] In the two years since ACMA's June 2021 report, there have been numerous mainstream media reports of serious injuries sufferers have attributed to Covid-19 vaccines. Prior to its official acknowledgement by the government and mainstream media, any social media discussion of vaccine injuries was likely judged "anti-vaccination" "misinformation" by ACMA. If ACMA had possessed the proposed powers at this time, social media discourse on vaccine injuries would have likely been censored at ACMA's direction. ACMA's researchers conducted a "representative survey" of 2,659 Australians, dividing them into either "informed" or "misinformed" based on whether they "agreed with official advice at the time" regarding "COVID-19 guidelines, prevention strategies and treatments". Any Australian who suffered an injury they attributed to a Covid-19 vaccine, prior to the government's "official" acknowledgement of the issue, would likely have been deemed "misinformed" by ACMA.

These two examples demonstrate that ACMA's judgement of what is misinformation, and what is not, is fallible. ACMA's own report admitted: "Given the constantly shifting nature of misinformation, *difficulties in assessing falsehoods*, and the challenges in accessing relevant data, it is not possible to quantify the true scale and volume of misinformation in Australia." (Emphasis added) Despite this admission, the government is proposing to make ACMA the arbiter of online truth.

[2] Rachel Eddie, "'You couldn't eat it': Food for tower residents left in corridors as deliveries delayed", The Age, 6 July 2020

[3] Mary Ward, "Thousands left waiting for compensation after claims of COVID-19 vaccine injury", Sydney Morning Herald, 16 April 2023

3. Government and mainstream media cannot be deemed "misinformation"

The proposed Bill claims to balance freedom of expression with the need to address online harm, by outlining a number of exceptions, which includes "professional news content and authorised electoral content" and "content authorised by the Commonwealth, State or Territory governments". This means that content produced by mainstream media or authorised by the government cannot be considered misinformation.

An examination of mainstream media allegations and claims from government representatives over the last several decades proves that both entities are fully capable of lying to the public, or providing false information, which has led to Australia's shameful involvement in several wars.

3.1 First Gulf War

The 11 October 1990 LA Times headline blared: "Witnesses Tell of Iraqi Atrocities in Kuwait: Congress: Members are shaken by what they hear. Kuwait's ambassador warns that 'time is running out.'" It reported testimony given to the US Congress by a 15-year-old eyewitness that "Iraqi soldiers with guns" had removed Kuwaiti "babies from the incubators … leaving the babies to die on the cold floor". It was entirely made up—the 15-year-old "witness" hadn't even been in Kuwait; she was the daughter of Kuwait's ambassador to Washington.

3.2 Iraq invasion

As is now proven, the lead-up to the 2003 invasion of Iraq saw lie after lie repeated in media headlines.

2001 New York Times: "Iraqi Tells of Renovations at Sites For Chemical and Nuclear Arms";
2002 CNN: "Experts: Iraq has tons of chemical weapons";
2002 The Star: "Mad Saddam ready to attack: 45 minutes from a chemical war";
2002 The Sun: "Brits 45 mins from doom";
2002 New York Times: "US Scoffs at Iraq Claim of No Weapons of Mass Destruction";
2003 Baltimore Sun: "CIA said Iraq had nuclear program".

Worldwide, thousands of media headlines faithfully repeated the same lies. The British and American liars got the war, destroyed the country and the region—and got away with it.

Australian politicians and government representatives also made false claims which facilitated Australia's participation in the illegal invasion of Iraq. On 20 March 2003 then-Prime Minister John Howard gave a televised address to the nation announcing his decision to commit Australian troops to the invasion of Iraq. The reasons Howard gave in that speech for supporting the war proved to be lies, including the main pretext of weapons of mass destruction, which Iraq didn't have (as proved later but which weapons inspectors had already insisted). He also made this claim: "This week the Times of London detailed the use of a human shredding machine as a vehicle for putting to death critics of Saddam Hussein. This is the man, this is the apparatus of terror we are dealing with", he said. "The removal of Saddam Hussein will lift this immense burden of terror from the Iraqi people." We now know—after launching a war that would kill a million Iraqis and set in train the events that unleashed the ISIS terror monsters on Iraq and Syria—the human shredding machine didn't exist either.

Former Labor Prime Minister Kevin Rudd, 15 October 2002: "Saddam Hussein possesses weapons of mass destruction … That is a matter of empirical fact.”

Former Liberal Prime Minister John Howard, 4 February 2003: “The Australian government knows that Iraq still has chemical and biological weapons and that Iraq wants to develop nuclear weapons. … The intelligence material collected over recent times, to which Australia has contributed, points overwhelmingly to Saddam Hussein having acted in systematic defiance of the resolutions of the Security Council, maintained his stockpile of chemical and biological weapons and sought to reconstitute a nuclear weapons program.”

Former Liberal MP Alexander Downer, 18 March 2003: “Iraq's weapons pose a grave threat to international peace and security and to Australia's national interests. … the world faces a threat which is terrible to contemplate: weapons of mass destruction in the hands of a ruthless dictator … Locating, securing and disposing of Iraq's weapons of mass destruction capabilities must and will be a major objective for the coalition. We must achieve the disarmament of Iraq.”

In 2003, Australian Ambassador Richard Butler, former head of the UN Special Commission to disarm Iraq from 1997 to 1999: “Iraq certainly did have weapons of mass destruction. Trust me. I held some in my own hands.”

3.3 Libya ‘intervention’

The world witnessed a repeat in Libya in 2011, when Qaddafi was accused of mass-rape and planning genocide against the rebels based in Benghazi:

The Guardian: “Gaddafi ‘supplies troops with Viagra to encourage mass rape’, claims diplomat”;
Washington Times: “Rebels say Gadhafi uses rape as fear tactic in war”;
CNN: “Libyan rebels say captured cell phone videos show rape, torture”.

In 2016, the UK House of Commons Libya Report acknowledged the 2011 intervention by the USA, UK, and France to “protect” Libyan civilians from “genocide”—which had resulted in the brutal murder of Qaddafi and the collapse of Libya into a failed state and haven for slave-traders and terrorists—had been a mistake: “This policy was not informed by accurate intelligence”, it stated. “In particular, the Government failed to identify that the threat to civilians was overstated and that the rebels included a significant Islamist element. … The result was … widespread human rights violations … and the growth of ISIL in North Africa.” (Emphasis added.)

3.4 China

Today, the Australian Citizens Party is gravely concerned that Australia’s mainstream media and certain politicians have promoted similarly false narratives against the Chinese government, to drive Australia toward an insane war with our largest trading partner, China. Our AUKUS partners, the US and UK governments, have openly declared China a geopolitical adversary.

The ACP has expended considerable effort towards investigating, and ultimately discrediting, many of the allegations against the Chinese government which have been levelled by mainstream media and politicians seemingly bent on war. The ACP’s research openly contradicts many mainstream media narratives and statements made by anti-China politicians—if ACMA’s proposed powers are legislated, would ACMA determine the ACP’s research “misinformation”, thereby resulting in the censorship of the ACP’s anti-war views from social media?

4. Social media censorship long-desired by intelligence agencies

When the government justified the proposed Bill, it emphasised the misinformation and disinformation that circulated the internet during COVID, citing as its example the claim early in 2020 that 5G radiation caused COVID, which led to 5G towers in Australia and around the world being vandalised. The truth, however, is that the Australian government and its closest geopolitical "partners" in the so-called Five Eyes countries— the USA, UK, Canada, and New Zealand—have been pushing for social media censorship powers since at least 2018.

As the ACP revealed in a 28 May 2019 release, "'Christchurch Call' establishes dangerous pretext for state censorship", the global agenda for a "techno-Stasi police state" has been set by the Five Eyes intelligence-sharing (a.k.a. surveillance) alliance. The ACP highlighted how an "August 2018 Five Eyes Ministerial gathering on Queensland's Gold Coast took aim at 'faster identification and removal of illicit content', and limiting 'coercive acts of interference and disinformation'." On 15 May 2019 New Zealand Prime Minister Jacinda Ardern and French President Emanuel Macron launched their "Christchurch Call" for internet censorship, in response to the Christchurch massacre; previously reluctant, the world's biggest social media platforms all signed on. In the COVID years, those social media companies entered into informal arrangements with government agencies to aggressively police content on their platforms; with this bill, the Albanese government is trying to make those arrangements formal, and permanent. As the ACP questioned in its 2019 release: "Identifying and removing illicit content featuring acts of terrorism, child sexual abuse and extremist violence is one thing, but who decides what constitutes 'disinformation'?" That is the age-old question.

The Australian Citizens Party has documented that social media companies are working in collaboration with intelligence-connected organisations to conduct mass censorship of alternative voices, under the guise of combating foreign interference and misinformation.[4] Numerous independent media publications have exposed social media companies' propensity to act as a censorship arm of the US government. Documents leaked by whistleblower Edward Snowden, a former contractor to the US National Security Agency (NSA), revealed that Five Eyes intelligence agencies worked with Big Tech to conduct mass internet surveillance.

5. Case study: ACP targeted for censorship

It is evident that the proposed Bill goes much further than stopping vandalism of 5G towers, or live-streaming atrocities, into areas open to political debate, including the public health response to COVID-19, supposed foreign interference in elections, and "undermining" democracy.

The government's fact sheet accompanying the exposure draft of the Bill states: "Misinformation and disinformation spread via digital platform services is a major issue worldwide. The rapid spread of false, misleading and deceptive information online has resulted in a multitude of harms from disrupted public health responses to *foreign interference in elections* and the *undermining of democratic institutions*." (Emphasis added)

Allegations of "cyber-enabled foreign interference" and "state-linked information operations" (i.e. misinformation) have already been used by the private sector to censor social media. ACP has identified a global censorship network, involving Big Tech, intelligence-connected organisations, and Western

[4] See attached, 'ASPI central in global censorship network'

think tanks, which uses accusations of state-backed inauthentic activity to silence undesirable views. As reported by *The Grayzone* on 2 November 2021, one week before the November 2021 Nicaraguan elections, social media giants Facebook, Twitter, YouTube (Google), and Instagram launched a massive censorship sweep of social media accounts, including media outlets, journalists and activists, which supported the left-wing Sandinista government. Facebook refused to distinguish between real people and alleged spam accounts, justifying mass account deletions by claiming that all were state-backed bots. Nicaragua has previously been subject to US government attempts to destabilise the country, which included a 2018 US-backed coup which attempted the violent overthrow of the Sandinista government.

If ACMA's proposed powers were in place in 2002, when the US, UK and Australian governments lied about Iraq having weapons of mass destruction, they could have been used to suppress public opposition to invasion and war. Will the ACP be de-platformed for saying the government is lying about the "threat" of Russia and China? The ACP has already been targeted for censorship under the proposed Bill, by the Australian Strategic Policy Institute (ASPI), an organisation which is funded by the Australian government, and is a major proponent of the alleged "threat" China and Russia pose to Australia.

The Australian Strategic Policy Institute presents itself as an "independent, non-partisan" policy think tank, despite evidence of its overwhelming bias towards the geopolitical interests of the United States and other Five Eyes nations. ASPI has been the primary agitator against the Chinese government, and is leading the insane drive to war with China. ASPI's funding sources, however, prove that its so-called "independence" is a farce. The majority of ASPI's funding comes from the Australian federal government, but ASPI also receives fund from foreign governments, primarily the US government; the private sector; and the arms industry. ASPI has received significant funding from social media giants Google, Facebook, and Twitter. A 1 April 2021 article by Marcus Rubenstein for *APAC News* documented that, since its founding in 2001, ASPI's defence industry sponsors have raked in over $51 billion in Australian government contracts.

ASPI has produced volumes of reports which accuse the Chinese government of interfering in Australian politics and civil society. These reports are often funded by the US government, which has deemed China a strategic adversary. For several years, ASPI has repeatedly accused the Chinese government of conducting foreign interference operations against Australia. However, ASPI's dubious "research" has been consistently discredited by the Australian Citizens Party and other researchers.[5] The ACP has repeatedly called out ASPI's appallingly low evidentiary standards and poor quality research, including asserting that in ASPI's anti-China reports, "relevant information is ignored, and sources are interpreted in extreme bad faith, or are misrepresented in a manner so misleading it can only be described as academic fraud." It is evident that the ASPI, which former Prime Minister Paul Keating has described as "a US cell" in its promotion of war with China, functions as a vehicle by which the US government can pursue its geopolitical objectives against China.

5.1 Cyber-enabled foreign interference allegations

The latest iteration of ASPI's Chinese influence hysteria is "cyber-enabled foreign interference", or "state-backed information operations", which are ostensibly conducted through social media platforms. ASPI alleges that foreign governments—invariably those targeted by Anglo-American strategic

[5] See attached, "ASPI's 'cyber-interference' allegations: more junk research"

agendas—have used social media to interfere in (primarily Western) elections. ASPI's allegations are overwhelmingly sourced to Western mainstream media publications and think tanks, and intelligence-connected organisations. To make these sensational claims, ASPI has relied on hearsay and has demonstrated very poor evidentiary standards. ASPI typically hedges its allegations with qualifiers such as "potentially", "might have", "possibly", "suggests". In one example, ASPI claimed that an example of election interference included mainstream media claims that in 2017, persecuted Australian journalist and founder of Wikileaks, Julian Assange, had acted as the "principal international agitator" in the lead up to the Catalan independence referendum, because Assange criticised the Spanish government on Twitter. ASPI wrote that Assange was allegedly "promoted and amplified by Russian state-sponsored media outlets and Twitter bots".

ASPI admits that it makes "inferences" to determine who is behind various social media "bots"—automated software which engages on social media, usually using fake accounts which mimic real people—which ASPI typically attributes to the Chinese government. ASPI claims that these "cyber-enabled foreign interference" operations seek to influence elections, "manipulate the information environment" (i.e. "misinformation") and "diminish public trust in democratic processes" (i.e. "undermine democratic institutions"), activities which, under the proposed law, would come under ACMA's purview.

ASPI is funded by social media companies and has been appointed one of a few select "research partners" which help social media giants decide whether bot accounts are "state-backed information operations". ASPI works closely with Twitter to provide analysis to support Twitter's mass purges of accounts deemed to be Chinese state-backed information operations, and has received funding from Twitter for this work. However, ASPI has admitted that it did not have access to Twitter's relevant data to independently verify whether accounts were actually linked to the Chinese government. Facebook's parent company, Meta, is also a major sponsor of ASPI and works with the think tank to analyse alleged state-backed information operations.

ASPI is not a disinterested or neutral party—it is funded by social media companies, weapons manufacturers, and the US government. ASPI's "research" on alleged Chinese state-backed social media information operations relies on analysis conducted by intelligence-connected organisations, which invariably attributes foreign influence "bots" to adversaries of the US government.[6]

5.2 ASPI targets the Australian Citizens Party

In a 24 July 2023 article titled "China's cyber interference narrows in on Australian politics and policy", ASPI analysts alleged that Chinese state-backed social media "bots" were interfering in Australia's domestic and foreign policies. ASPI claimed these bots criticised Australian spy agencies, AUKUS, the US-Australian alliance, and ASPI itself; and promoted the views of "certain individuals", naming former Prime Minister Paul Keating and the Australian Citizens Party (ACP), who are outspoken critics of ASPI's warmongering against China.

According to ASPI, this Chinese government misinformation operation included "amplifying division" over the Aboriginal "voice" debate, and "sustained targeting" of "the big four banks". "Major Australian banks are a key focus for many accounts in the campaign, including the Commonwealth Bank, the National Australia Bank, ANZ and Westpac", ASPI asserted. "This includes claims that Australian banks

[6] See attached, "ASPI central in global censorship network"

aren't serving regional Australia and First Nations customers. Concurrently, the campaign promotes the views of certain individuals (such as former prime minister Paul Keating) and organisations (*especially the Australian Citizens Party*)." (Emphasis added.) This followed similar allegations of November 2022, when ASPI announced that an alleged Chinese state-backed bot network was engaging in "more direct interference in Australia politics" and "seeking to engage in political interference" by "seeking to drive online attention" toward the social media accounts of the ACP and its members. ASPI's "analysis" came dangerously close to suggesting that those with views critical of AUKUS, intelligence agencies, and the US government, are part of a Chinese government foreign influence operation.

ASPI called for this alleged Chinese state-backed activity to be included in the government's bill to censor social media: "If the new ACMA powers to combat misinformation and disinformation, or a variation of the bill, are passed, then as a first step ACMA should mandate that digital platforms, including social media platforms, disclose all state-backed influence operations publicly …"

ASPI's allegations that the Australian Citizens Party's social media accounts are being amplified by an alleged Chinese-state backed information are alarming. ASPI exerts powerful influence on Australian government policy-making, and already functions as a key player in a global censorship network which conducts mass censorship of social media accounts which ASPI deems are "state-backed information operations". ACMA's June 2021 report, which informed the proposed Bill, proposed that the government make ASPI's censorship activities official. Recommendation 5 of the ACMA report states that "the government should consider establishing a Misinformation and Disinformation Action Group to support collaboration and information-sharing between digital platforms, government agencies, researchers and NGOs on issues relating to disinformation and misinformation". If the government implements ACMA's recommendation, ASPI will likely play a central role in deciding whether the social media activities of those opposing the interests of ASPI's funders (which include major arms manufacturers and the US government), such as the Citizens Party, are part of alleged Chinese government "misinformation" campaigns, thereby facilitating the censorship of alternate views and silencing genuine political discourse.

6. Case study: Foreign influence peddlers a conduit of US government foreign influence?

Allegations that social media platforms have facilitated misinformation or foreign interference can be used to attack specific companies, to the benefit of their corporate competitors or the strategic interests of Western governments. Often, conflicts of interests are not disclosed by those making such allegations.

In December 2019, the Morrison government "requested that major digital platforms in Australia develop a voluntary code of practice to address online disinformation and news quality concerns". ACMA was tasked with overseeing the development of the code and reporting on the "adequacy of digital platforms' disinformation and news quality measures". ACMA's resulting June 2021 report informed the government's proposed disinformation laws and new powers for ACMA.

A month prior to the Morrison government's request, Labor politicians launched a corresponding arm of potential censorship, via theI"Foreign interference through Social Media" inquiry. After the lapse of the previous parliament, the inquiry was re-launched by Liberal Senator James Paterson in November 2022.

From inception, ASPI's influence over both iterations of the inquiry was evident. ASPI's testimony, submission and research were frequently referenced by both iterations of the inquiry, and the hearings were stacked with ASPI associates. For example, in addition to current and former ASPI staffers, witnesses to the inquiry included:

- The Alliance for Securing Democracy, which operates under the German Marshall Fund, an ASPI corporate sponsor.
- Badiucao, an artist who produces the artwork for many of ASPI's reports which attack China.
- Google, Twitter, and Facebook, which are all funders of ASPI.
- CyberCX, one of ASPI's corporate sponsors.
- The Stanford Internet Observatory, a speaker at ASPI's 2023 Sydney Dialogue, which participates with ASPI in working with social media companies to censor alleged "state-backed" accounts.

When Liberal Senator James Paterson resurrected the inquiry, which he then chaired, it was evident that Paterson's aim was to use it as a vehicle to attack the Chinese government and to pursue Paterson's personal vendetta against social media platform, TikTok. TikTok's parent company, ByteDance, is Chinese-owned. Numerous witnesses who were invited to testify before the inquiry had previously published reports attacking TikTok, such as Internet 2.0, an organisation which counts numerous former US government officials as part of its leadership team.

Although the final report and hearings of the inquiry were replete with claims of alleged Chinese and Russian government foreign interference, it appears that the inquiry itself was a conduit of American government interference.

For example, Paterson re-launched the "Foreign Interference through Social Media" inquiry shortly after his return from Washington DC, where he attended a September 2022 conference of UK-based organisation, the Inter-Parliamentary Alliance on China (IPAC), of which Paterson is a co-chair. Paterson's trip was funded by IPAC. IPAC's Members are composed of international parliamentarians, including Australian politicians, whose primary objective is to agitate in their respective countries against the Chinese government. IPAC has initiated an international "series of coordinated legislative actions" and "parliamentary interventions" to ensure that IPAC-favoured (and usually anti-China) legislation is introduced; and, after intense media campaigns and lobbying by IPAC Members, is often passed.

French and British parliamentary members of IPAC have led attacks against TikTok in their respective countries, successfully lobbying their governments to have the company banned from government devices. IPAC co-chair Senator James Paterson led the charge for TikTok to be banned from government devices in Australia. IPAC members served as witnesses to the hearings of the Australian Foreign Interference through Social Media inquiry. IPAC is funded by the National Endowment for Democracy (NED), the notorious US government-funded regime-change proponent (one of the NED's co-founders admitted that much of the agency's activities were formerly conducted covertly by the CIA). The US has been at the forefront of campaigning against TikTok, including funding ASPI's 2020 report which claimed that TikTok was "curating and controlling global information flows", under direction of the Chinese government.

In a 20 April 2023 interview with the ABC, Paterson was asked about members of the US Federal Communications Commission who had been very outspoken in demanding a total ban on TikTok. Paterson replied that he "was in the United States personally only a few weeks ago to discuss this with legislators and members of the administration". Paterson's March-April trip to Washington DC to participate in a "bipartisan AUKUS defence industry delegation", was courtesy of Pyne and Partners, the consultancy firm of former Defence Minister Christopher Pyne, which promotes AUKUS. The US is considering a total ban of TikTok and forcing TikTok's parent company, ByteDance, to divest TikTok to a non-Chinese owner. The final report of Paterson's inquiry recommends that, if the US government does undertake these actions, Australia should follow suit. Commissioner Brendan Carr of the US Federal Communications Commission, whom Paterson described as "one of the earliest and leading voices in calling out the risks" allegedly posed by TikTok, testified before the inquiry.

Paterson evidently personally consulted with members of the US government while chairing a parliamentary inquiry into foreign interference conducted through social media. This inquiry was transparently aimed at attacking the Chinese government and TikTok, in alignment with US strategic objectives. This example demonstrates that allegations of misinformation and foreign interference through social media can be weaponised to serve the interests of entities such as TikTok's competitors (the social media companies which fund ASPI), and the US government.

7. Conclusion

It appears that ACMA's proposed powers will enable censorship under the guise of preventing alleged election interference or undermining democratic institutions. Sensationally hyping so-called "state-linked information operations" on social media provides valuable media fodder and justifies mass purges of accounts, as genuine users with undesirable views can be deleted along with alleged state-backed bots. It also provides "evidence" to push for policy change—for example, the hearings of the current parliamentary inquiry into Foreign Interference through Social Media were stacked with ASPI associates. The alleged threat of foreign interference through social media also allows for guilt-by-association attacks—such as ASPI's claim that the Chinese government is covertly promoting the Australian Citizens Party's social media accounts. If ACMA's proposed powers are legislated, would the ACP be censored as a result of ASPI's allegations?

The ACP accepts that social media is rife with misinformation and disinformation; but the only way to combat it is to publicly refute it, not censorship. Thinkers have struggled with the implications of free speech for centuries, and concluded that limiting speech is far more dangerous to society than the regrettable consequences of false claims. That's why free speech is enshrined in the First Amendment of the Bill of Rights in the US Constitution: "Congress shall make no law ... abridging the freedom of speech, or of the press". And why it is enshrined in Article 19 of the Universal Declaration of Hu- man Rights, which Australia helped to draft in 1948: "Every- one has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (Emphasis added.)

Social media is a double-edged sword: it can be a channel for the worst misinformation and disinformation, but so can governments, as we have witnessed; alternatively, it can also be the medium that exposes government and corporate lies that the corporate mainstream media won't, which restores power to the people. Regulating truth on social media will not protect democracy, it will suppress it.

Denounce Albanese’s Orwellian social media censorship law

18 July—*Australians have until 6 August to make submissions objecting to the government’s bill to regulate truth on social media. See submission details below.*

The Albanese government’s Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 is another dangerous lurch down the path to totalitarianism which all Australians should oppose. The bill gives the government power to regulate “truth” online by being able to force social media platforms to censor “misinformation” and “disinformation” that is “harmful”—three vague terms that are open to very broad interpretation. Until 6 August, Australians have the opportunity to make submissions to the government’s consultation process on the exposure draft of the bill, to send a powerful message that such interference with free speech is unacceptable.

Watch Australian Citizens Party Research Director Robert Barwick discuss the implications of this bill on Martin North’s “Walk The World” YouTube channel: It’s 21 Days to 1984!

Pretext

When the government justifies this law, it emphasises the misinformation and disinformation that circulated the internet during COVID, citing as its example the claim early in 2020 that 5G radiation caused COVID, which led to 5G towers in Australia and around the world being vandalised. The truth, however, is that the Australian government and its closest geopolitical “partners” in the so-called Five Eyes countries—the USA, UK, Canada, and New Zealand—have been pushing for social media censorship powers since at least 2018.

As the ACP revealed in a 28 May 2019 release, “‘Christchurch Call’ establishes dangerous pretext for state censorship”, the global agenda for a “techno-Stasi police state” has been set by the Five Eyes intelligence-sharing (a.k.a. surveillance) alliance. The ACP highlighted how an “August 2018 Five Eyes Ministerial gathering on Queensland’s Gold Coast took aim at ‘faster identification and removal of illicit content’, and limiting ‘coercive acts of interference and disinformation’.” On 15 May 2019 New Zealand Prime Minister Jacinda Ardern and French President Emanuel Macron launched their “Christchurch Call” for internet censorship, in response to the Christchurch massacre; previously reluctant, the world’s biggest social media platforms all signed on. In the COVID years, those social media companies entered into informal arrangements with government agencies to aggressively police content on their platforms; with this bill, the Albanese government is trying to make those arrangements formal, and permanent. As the ACP questioned in its 2019 release: “Identifying and removing illicit content featuring acts of terrorism, child sexual abuse and extremist violence is one thing, but who decides what constitutes ‘disinformation’?”

That is the age-old question.

Suppressing, not protecting, democracy

The government’s justification in its own fact sheet accompanying the exposure draft of the bill illustrates its inherent dangers. It states:

“Misinformation and disinformation spread via digital platform services is a major issue worldwide. The rapid spread of false, misleading and deceptive information online has resulted in a multitude of harms from disrupted public health responses to foreign interference in elections and the undermining of democratic institutions.”

The omnipresent image of Big Brother, from the film *1984*.

Straight away, it’s clear this bill goes much further than stopping vandalism of 5G towers, or live-streaming atrocities, into areas open to political debate, including the public health response to COVID-19, supposed foreign interference in elections, and “undermining” democracy.

The fact that the bill explicitly exempts any government communication, of any level of government, from being considered misinformation or disinformation, shows how Orwellian this law will be. While the bill’s penalties won’t apply to individuals, it will enforce a regime of suppression of any speech on social media that undermines government claims.

It would not just apply to protecting public health, as we have already witnessed in the mass-censorship of contrary analysis relating to COVID-19, including of qualified doctors and scientists. It would also apply to debates on foreign policy, such as whether Russia or China are “threats” to Australia, which the government claims to justify committing almost $1 billion to arming NATO’s proxy Ukraine against Russia, or promising $368 billion to buy US and British submarines to deploy against China.

Will the ACP be de-platformed for saying the government is lying about Russia and China? If these powers were in place in 2002, when the US, UK and Australian governments lied about Iraq having weapons of mass destruction, they could have been used to suppress public opposition to invasion and war.

Stick to the principle

The ACP accepts that social media is rife with misinformation and disinformation; but the only way to combat it is to publicly refute it, not censorship. Thinkers have struggled with the implications of free speech for centuries, and concluded that limiting speech is far more dangerous to society than the regrettable consequences of false claims. That’s why free speech is enshrined in the First Amendment of the Bill of Rights in the US Constitution: “Congress shall make no law … abridging the freedom of speech, or of the press”. And why it is enshrined in Article 19 of the Universal Declaration of Human Rights, which Australia helped to draft in 1948: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media* and regardless of frontiers." (Emphasis added.)

Social media is a double-edged sword: it can be a channel for the worst misinformation and disinformation, but so can governments, as we have witnessed; alternatively, it can also be the medium that exposes government and corporate lies that the corporate mainstream media won't, which restores power to the people.

Regulating truth on social media will not protect democracy, it will suppress it.

What you can do

Make a submission immediately—the deadline is 6 August.

A "submission" does not need to be a lawyer's analysis; it's simply a letter from you, as brief or as long as you like, stating your strong objection to the bill, and why.

Visit the government's exposure draft consultation website, which has instructions for uploading or emailing submissions.

Documentation: the ACMA social media censorship bill and its Orwellian implications

By Bob Butler

The Australian Government has released a draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 ("the Bill") by which it claims to "keep Australians safe online". Minister for Communications Michelle Rowland claimed: "The Albanese Government is committed to keeping Australians safe online, and that includes ensuring the Australian Communications and Media Authority (ACMA) has the powers it needs to hold digital platforms to account for mis and disinformation on their services."

The Bill has been introduced following the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry in 2019, which highlighted the significant risks posed by the "infodemic" of misinformation and disinformation shared on digital platforms, and after the introduction of the Government-requested voluntary code of conduct for disinformation and news quality by certain digital platform services. The proposed powers implement the key recommendations in ACMA's June 2021 report to government on the adequacy of digital platforms' disinformation and news quality measures.

Under the Bill, ACMA (established by the *Australian Communications and Media Authority Act 2005*) would be granted new and enhanced powers to combat allegedly harmful misinformation and disinformation online, and to impose significant financial penalties for non-compliance with the new restrictions. The Bill proposes to insert its provisions into the Commonwealth's *Broadcasting Services Act 1992* as a new schedule of provisions related to digital platform services.

ACMA would be granted the power to compel digital platforms to maintain records related to misinformation and disinformation and these records would have to be handed over upon request. ACMA would have the authority to request that digital platform service providers prepare a voluntary "code of practice" for the industry, outlining strategies to combat misinformation.

Companies failing to adhere to this code could be subject to penalties of up to $2.75 million or two per cent of their global turnover, whichever is higher. Finally, ACMA would be able to establish and enforce its own industry standard. Violations of this standard could lead to companies being fined up to $6.8 million or five per cent of their global turnover. ACMA's powers would extend to various online platforms, including social media, news-aggregators, and podcasts. ACMA would not have the authority to remove individual pieces of content, and the new powers would not apply to certain excluded content including professional news content.

Minister Rowland: "Mis- and disinformation sows divisions within the community, undermines trust and can threaten public health and safety".

The Bill defines "misinformation" and "disinformation" as follows (with the key difference being "intent"):

- "misinformation" is online content that is false, misleading or deceptive, that is shared or created without an intent to deceive, but that is reasonably likely to cause or contribute to serious harm. [S7(1)]
- "disinformation" is a subset of misinformation that is disseminated deliberately or with an intent to deceive or cause serious harm. [S7(2)]

For misinformation to be covered by the Bill, it must be "reasonably likely that it would cause or contribute to serious harm". For harm to be serious, it is intended that it must have severe and wide-reaching impacts on Australians. Examples provided in the Bill include inciting hatred, vandalising critical communications infrastructure, serious financial or economic harm or serious harm to the health of Australians. It would appear to be focused on misinformation shared socially, rather than professionally—for example, "conspiracy theories" rather than information that is accidentally incorrect despite a publisher's best intentions.

The Bill defines the "digital platform services" to which it applies and takes a three-layered approach to defining the "digital platform services" that are within the scope of its powers. These services are broadly defined [S4(1)], referring to digital services that:

1. collate and present content from a range of online sources (content aggregation services) [search engines, websites];
2. enable online interaction between multiple end-users (connective media services) [Facebook, Twitter etc.];
3. provide audio-visual or moving visual content to end-users (media sharing services) [YouTube, Rumble, Bitchute etc.]; and
4. other digital services specified by the Minister.

As a result, a significant category of broad digital platforms and digital platform service providers will be within the scope of the Bill—ranging from social media channels to search engine sites and peer-to-peer marketplaces. However, digital services will not be captured to the extent that they are internet, SMS or MMS service providers. [S4(1)(e)-(f)]

In claiming to balance freedom of expression with the need to address online harm, the Bill outlines a number of exceptions, including:

1. content produced in good faith for entertainment, parody or satire;
2. professional news content and authorised electoral content;
3. content authorised by the Commonwealth, State or Territory governments; and
4. content produced by or for accredited education providers.

The Bill also requires that in determining whether or not to register a voluntary code, ACMA consider: (i) whether the code burdens freedom of political communication; and (ii) if so, whether the burden is reasonable and not excessive, having regard to any circumstances the ACMA considers relevant" [S37(d)]. A similar requirement applies in respect of a "Standard" (in effect a compulsory code) which ACMA proposes to issue [S40(d)].

The Bill also provides in relation to freedom of political communication:

60 Implied freedom of political communication

(1) The provisions of:

(a) this Schedule; and

(b) the digital platform rules; and

(c) any misinformation code registered under Part 3; and

(d) any misinformation standard;

have no effect to the extent (if any) that their operation would infringe any constitutional doctrine of implied freedom of political communication.

Digital platforms currently self-manage approaches to misinformation or disinformation. This may take the form of collective industry codes of practice, such as the DIGI disinformation code of practice—a code that major technology companies such as Microsoft, Twitter, TikTok and Google have signed up to in recognition of their "role as important actors within the Australian information ecosystem".

The Bill gives ACMA the power to step in where industry-led self-regulation is determined by ACMA as inadequate, or where ACMA considers that it fails to remedy misinformation and disinformation. Specifically, the proposed powers would enable ACMA to:

1. gather information from, or require digital platform providers to keep records about matters regarding misinformation and disinformation; [S14]

2. publish information on its website relating to misinformation or disinformation regulation, measures to combat this issue, and the prevalence of such content—both on individual platforms and at an industry level; [S25-28]

3. request the industry develop "misinformation codes"—codes of practice covering measures to combat misinformation and disinformation (that ACMA could then register and enforce); [S29-44] and

4. create and enforce "misinformation standards"—industry standards (a stronger form of regulation than a code of practice) where ACMA deems a code of practice is ineffective. [45-56]

Notably, ACMA will not have the power to request specific content or posts to be removed from digital platforms or have a role in determining what is considered truthful. Digital platforms continue to be responsible for the content they host and promote to users.

This purports to recognise the challenging balance between the desire to ensure free speech online; the role of digital platform providers in determining, and being responsible for, the quality and nature of content on their own platforms; and the safety risks posed by certain forms of online content—such as those already regulated by the eSafety Commissioner.

Further, ACMA will not be able to use its powers in relation to private messages [Ss 14(3), 19(4), 34]—save for, perhaps, its information-gathering powers to ensure service providers collect information about key risks.

Nonetheless, it is clear that the proposed legislation is designed to reserve the ability for ACMA to force platforms into line where self-regulatory codes and practices have failed.

Penalties

Digital platforms that do not comply will face substantial penalties—up to, the greater of, AUD$6.88 million or 5 per cent of global turnover for corporations (in recognition of the size of digital service providers), and up to $1.38 million for individuals [Inserted as S205F(5H) into the *Broadcasting Services Act 1992* (Cth)]. This is in addition to warnings, remedial directions and other "softer" remedies available at ACMA's discretion.

ACMA, like many other instrumentalities, is structured to be independent of, and not accountable to, Government. Section 15 of the *Australian Communications and Media Authority Act* provides:

15 ACMA not otherwise subject to direction

Except as otherwise provided by or under this or any other Act, the ACMA is not subject to direction by or on behalf of the Commonwealth.

Section 14 of the *Australian Communications and Media Authority Act* provides the only Ministerial control mechanism in the Act, in these ambiguous terms, providing:

14 Minister may give directions to ACMA

(1) The Minister may give written directions to the ACMA in relation to the performance of its functions and the exercise of its powers.

(2) However, such a direction can only be of a general nature if it relates to:

(a) the ACMA's broadcasting, content and datacasting functions; or

(b) the ACMA's powers relating to those functions.

(3) A direction under subsection (1) must be published in the Gazette.

(4) The ACMA must perform its functions, and exercise its powers, in a manner consistent with any directions given by the Minister under subsection (1).

(5) This section does not affect the Minister's powers under the Broadcasting Services Act 1992 *to give directions to the ACMA*

Schedule 8 of the *Broadcasting Services Act 1992* in its summary states provides that "The ACMA may make online content service provider rules about gambling promotional content provided on an online content service in conjunction with live coverage of a sporting event."

Section 27 of Schedule 8 gives a further limited power of direction over ACMA for these limited circumstances:

27 Minister may direct the ACMA about the exercise of its powers

(1) The Minister may, by legislative instrument, give the ACMA a direction about the exercise of the powers conferred on the ACMA by this Schedule (other than Part 4 or 5). (Those Parts relate to complaints and enforcement).

What are the problems with the proposed legislation?

I agree with the opinion of David Coleman, Shadow Minister for Communications, that "this is a complex area of policy and government overreach must be avoided". He added: "[The] public will want to know exactly who decides whether a particular piece of content is misinformation or disinformation."

That is one of the serious issues with the proposed legislation. The Bill's vague definitions of "misinformation" and "disinformation" are open to interpretation and abuse by those making decisions about that interpretation, apart from the issue of who decides what is "misinformation" or "disinformation" and what is "harm".

As to the Bill overall, it has been noted that George Orwell wrote the book *Nineteen Eighty-four* in which a totalitarian government regulated the truth and that it is quite a coincidence that on Orwell's 120th birthday, the Australian

Government has announced that it would introduce legislation which heads down that path, here in Australia.

That comment is reinforced by Section 2 of the Bill in its definition of "excluded content for misinformation purposes means any of the following:

(e) content that is authorised by:

(i) the Commonwealth; or

(ii) a State; or

(iii) a Territory; or

(iv) a local government."

In other words, anything authorised by Government cannot be held to be misleading.

One only has to consider the Government position on the Iraq invasion, or during the COVID period or the background behind what is presently occurring in Ukraine—the government position cannot be classed as "misleading", unlike any position which opposes that Government line.

Discussion and opinions as to the Bill which focus on its aim to remove "misinformation" and "disinformation" from the internet, concentrate on the large providers such as the Digital Industry Group Inc. (DIGI) adopted by eight digital platforms—Google, Facebook, Microsoft, Twitter, TikTok, Redbubble, Apple and Adobe.

The Bill, however, is not limited to those large platform providers but extends to all digital platform providers, whatever their size, the summary in the Bill noting:

"The ACMA may make digital platform rules requiring digital platform providers to keep records and report to the ACMA on matters relating to misinformation and disinformation on digital platform services. The ACMA may obtain information, documents and evidence from digital platform providers and others relating to those matters. The ACMA may publish information relating to those matters on its website. Bodies or associations representing sections of the digital platform industry may develop codes in relation to measures to prevent or respond to misinformation and disinformation on digital platform services. If the ACMA registers a misinformation code, digital platform providers in the relevant section of the digital platform industry must comply with the code.

"Where there is no registered misinformation code, a registered misinformation code is deficient or there are exceptional and urgent circumstances, the ACMA may determine a standard to provide adequate protection for the community from misinformation or disinformation on digital platform services. Digital platform providers are required to comply with misinformation standards that apply to them."

The Bill has clearly given primary (if not sole) consideration to the largest platforms like Facebook, Reddit and Twitter etc. and yet has brought in-scope (intentionally or unintentionally) thousands and thousands of community websites that are part of the "social web" due to its broad definitions. The law is way too broad, and is not structured in any way to give regard to the size of platforms that it applies to.

A standard requiring small platform providers to keep records, hand over documents, attend to give evidence and to face enormous penalties for alleged breaches would be extremely onerous and concerning. In that regard it should be borne in mind that there are many websites that offer social features that come within the definition in S4 of the Bill of a digital platform service being a digital service that is a content aggregation service, a connective media service, a media sharing service or (the catchall phrase) a digital service specified by the Minister. Without any specific limitations on a Code, the Bill potentially gives the largest digital services in an industry the ability to not only write their own regulations in the form of a Code but for that Code in its terms to be such that it could damage their smaller competitors by their risking infringements and onerous regulatory requirements.

The EU has introduced this regulatory type of legislation (the *Digital Services Act*) but has defined large providers as VLOPs (Very Large Online Platforms) or VLOSEs (Very Large Online Search Engines) and they are treated separately by the European Commission.

George Orwell and his famous book about a government permanently at war, which regulates "truth."

If ACMA determines some content to be "misinformation" or "disinformation" it can at its option issue a warning, a remedial direction to the provider, or other "softer" remedies, or impose a penalty. The penalties are potentially huge and would quickly cause most companies or individuals to comply and exclude or remove the complained-of content or go out of business unless they chose to get involved in expensive Court proceedings to determine whether or not the material did fall within the definitions in the Bill.

There is no limitation in the Bill of what "standards" might be imposed by ACMA if it decided to issue a standard applying to particular suppliers (or all suppliers) rather than endorse a voluntary code.

The Bill is also expressed to apply extraterritorially, S12 providing:

12 Extra-territorial application

This Schedule extends to acts, omissions, matters and things outside Australia.

The requirements of the Bill are accordingly expressed to apply to any platform provider anywhere in the world. Any breach of this proposed new standard would see international tech giants liable to pay a steep maximum penalty with fines of up to $6.88 million (US$4.6 million) or 5 per cent of global turnover. For perspective, 5 per cent of Facebook's parent company Meta's global turnover amounts to approximately $8 billion (US$5.3 billion).

The alternative to such a reach would be to block platforms which did not comply with a code or standard, apparently a step too far for Government in relation to this Bill.

My general thoughts:

It is difficult to see how this legislation in its present form could be simply amended to make it workable without incorporating unacceptable risks of the *Nineteen Eighty-four*-type consequences.

It should not be administered by an unaccountable body but administration by the current political class would be of comparable concern.

If there is to be any limitation on content, it should be clearly and unambiguously defined. There are many obvious examples, we can all think of things that should not be broadcast, but it is difficult to define them in some general way. There should not be any definition which incorporates an ability to determine what is "truth".

There should be a capacity to have any such objectionable content removed by the service provider—perhaps with the sanction of blocking the site until it is removed. There should be a differentiation in the way smaller socially-oriented platform services are categorised and treated as opposed to the substantial international services.

Bob Butler is a solicitor and Member of the Australian Citizens Party's Committee of Management.

ASPI central in global censorship network

By Melissa Harrison

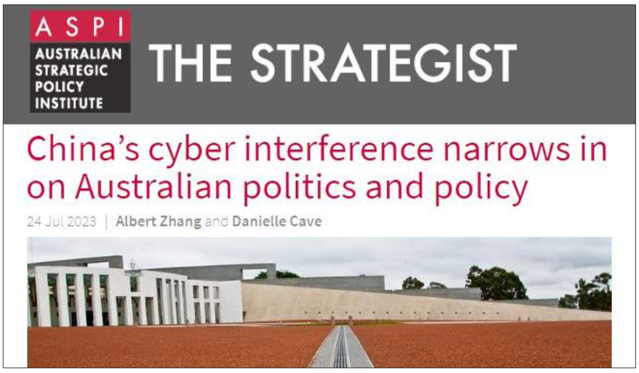
An Australian defence think tank which takes money from foreign governments is driving the push to censor supposed "foreign influence" operations on social media in Australia. The Australian Strategic Policy Institute (ASPI), which is funded by the US State Department, the British, Dutch and Japanese governments, and is heavily sponsored by multinational weapons manufacturers, is smearing the Australian Citizens Party (ACP) and its highly effective campaign against bank branch closures, as examples of "Chinese covert influence operations" which should be censored from social media. ASPI's attack on the ACP coincides with the Australian government's release of new legislation to censor alleged "harmful" "misinformation" and "disinformation" on social media, including information deemed foreign interference. The ironic but blatant truth is that ASPI is *the* principal foreign interference operation in Australia, manipulating Australian defence and foreign policy on behalf of its foreign funders, and is a key player in a US intelligence-directed global network that conducts mass-censorship operations to advance Anglo-American strategic objectives.

ASPI has repeatedly alleged that foreign governments—invariably those targeted by Anglo-American geopolitical agendas—have launched "cyber-enabled foreign interference" operations against Western democracies. But ASPI's "cyber-influence" research is funded by the US government, NATO, US "Big Tech" companies, and organisations such as the US/UK government-funded Institute for War and Peace Reporting (IWPR). IWPR also receives funds from the National Endowment for Democracy (NED), the notorious US government-funded promoter of "regime change" (one of NED's co-founders admitted that much of the agency's activities were formerly conducted covertly by the US Central Intelligence Agency).

ASPI claims that the Chinese government has conducted cyber-enabled foreign interference operations against Australia. However, ASPI routinely hedges its sensational allegations—ASPI's reports are replete with qualifiers such as "potentially", "might have", and "possibly". ASPI admits that it makes "inferences" to determine who is behind various social media "bots"—automated software which engages on social media, usually using fake accounts which mimic real people—which ASPI typically attributes to the Chinese government.

In a 24 July 2023 article titled "China's cyber interference narrows in on Australian politics and policy", ASPI analysts claimed to have identified a network of "coordinated inauthentic accounts", or bot accounts, which they assessed were "*likely* involved in an ongoing Chinese Communist Party influence and disinformation campaign targeting Australian domestic and foreign policies" (emphasis added). ASPI cautioned that this bot network amplified "negative messaging" around domestic spy agency the Australian Security Intelligence Organisation (ASIO) and criticised AUKUS, the US-Australian alliance, and ASPI itself.

ASPI claimed that this "CCP-linked information operation" promoted the views of "certain individuals", naming former Prime Minister Paul Keating and the Australian Citizens Party, who are prominent critics of ASPI, AUKUS and the drive to war with China. This followed similar allegations in November 2022, when ASPI announced that an alleged Chinese state-backed bot network was engaging in "more direct interference in Australian politics" by "seeking to drive online attention" towards the ACP and its members. ASPI's "analysis" came dangerously close to suggesting that all those with views critical of AUKUS, intelligence agencies, the US government, and ASPI itself, are automatically part of a Chinese government foreign influence operation. As discussed below, ASPI's tactic of implying guilt by association has previously been used by ASPI's global censorship fraternity to silence alternative voices.



A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

THE STRATEGIST

China's cyber interference narrows in on Australian politics and policy

24 Jul 2023 | Albert Zhang and Danielle Cave

ASPI's July attack on ACP campaigns as part of a Chinese "interference" operation. Photo: Screenshot

'Chinese bots' brought to you by US intelligence-linked organisations

The basis for ASPI's claim that an Australia-targeting bot campaign was a Chinese government operation, came down to ASPI's assessment that these bots were part a larger spam network dubbed "Spamouflage Dragon" (or "Dragonbridge"). ASPI claimed that the bots displayed "behavioural traits" which linked them to Spamouflage. The Spamouflage network has been deemed a Chinese state-backed operation by Big Tech and various intelligence-connected companies, although Google has admitted that only a "small fraction" of the Spamouflage network promotes "pro-China messages" and criticises the USA.

Social media companies readily admit that the Spamouflage network is ineffective as a propaganda operation, as its low-quality content has virtually zero organic engagement and has failed to gain any traction with real audiences. Nevertheless, Spamouflage has been sensationalised in Western media as a vehicle for covert Chinese government cyber-influence operations. The main producer of research which attributes Spamouflage activity to the Chinese government is an American cyber analytics company named Graphika, which describes itself as "the best in the world at analysing how online social networks form, evolve, and are manipulated". Graphika, which christened the Spamouflage network, is frequently referenced in Western mainstream media as an authority on cyber-influence operations. ASPI's reports and articles include numerous references to Graphika's research.

Although Graphika is ostensibly a private company, in reality, as documented in a 25 January 2022 exposé for online publication MintPress News, Graphika "operates as a front for the US deep state to control social media and delete accounts". US government records reveal that over the last three years, Graphika has received over US$7.8 million in funding from US defence agencies. Graphika's "research partners" include the Pentagon's Defence Advanced Research Projects Agency (DARPA); the US Select Committee on Intelligence; and the Minerva Initiative, a US Department of Defence-funded research organisation. Graphika's research partners also include the Institute for Strategic Dialogue, a NATO-funded organisation with ties to the aforementioned National Endowment for Democracy (NED). As documented by MintPress,

Continued page 9

ASPI central in global censorship network

From page 8

many Graphika staffers formerly worked for US intelligence and national security agencies, and numerous others were educated at King's College in London, the notorious "school for spooks" which is headed by former NATO, military and intelligence officials. Graphika staff also participated in the now discredited Institute for Statecraft's infamous "Integrity Initiative", which was exposed in 2018 as an international media and political influence operation to spread anti-Russian propaganda, covertly funded by the UK and US governments, NATO, and Facebook.

Graphika has partnered with online media giant Google to counter alleged Spamouflage activity. Graphika has also partnered with the Washington, DC-based Atlantic Council, a NATO- and US/UK government-funded think tank which effectively operates as an arm of NATO, on a number of joint projects to analyse social media bot activity. The Atlantic Council has extended its influence over social media companies through the work of its Digital Forensics Research Lab (DFRLab), which partnered with Facebook in 2018, ostensibly to identify and counter election disinformation and interference. This partnership gave DFRLab unprecedented power to curate the news items which Facebook users could see.

Graphika's intense focus on the Spamouflage network took off in April 2019 after the company appointed former NATO press officer and Integrity Initiative participant Ben Nimmo as its Head of Investigations. Nimmo was credited as the lead author of many of its reports on Spamouflage. Prior to joining Graphika, Nimmo was a non-resident senior fellow of the Atlantic Council's DFRLab, which he had co-founded. In February 2021, the Atlantic Council published an anonymous 26,000-word report titled "The Longer Telegram: Toward a new American China strategy", which effectively called for regime change in China.[1] One week later, Nimmo left Graphika to join Facebook as its Global Threat Intelligence Lead.

Graphika is not the only intelligence-connected organisation which attributes Spamouflage activity to the Chinese government. Since at least 2019, Google and Facebook have worked with cybersecurity firm Mandiant to identify and counter alleged Chinese and Russian cyber-influence activity. Mandiant, acquired by Google in 2022, was formerly a subsidiary of FireEye, a company which was launched with funding from In-Q-Tel, the CIA's investment arm, and counts the CIA as a client. ASPI's cyber-interference reports contain numerous references to Mandiant's research. Coincidentally, in June 2022 both ASPI and Mandiant simultaneously identified Spamouflage as the culprit behind an alleged Chinese state-backed information operation which targeted an Australian rare earths mining company.

In addition to ASPI's deep ties to the defence industry, ASPI's staff also have connections to the intelligence sector. This includes ASPI's Executive Director Justin Bassi, who was formerly Cyber Intelligence Mission Manager at the Office of National Intelligence (ONI), Australia's peak intelligence organisation. Bassi infamously wore CIA cufflinks inside the Australian Senate, while serving as an advisor to Attorney-General George Brandis. Other ONI alumni include Dr Alexandra Caples, director of ASPI's International Cyber Policy Centre, which has produced the majority of ASPI's cyber-influence reports. Another previous ONI staffer is former analyst and team leader of the ONI's Open Source Centre, Danielle Cave, who is now ASPI's director of Executive, Strategy & Research. Cave has co-authored many of ASPI's reports which allege that the Chinese government is conducting cyber-enabled foreign influence operations. Cave's work includes the aforementioned articles which claimed that a Chinese state-backed bot network was promoting the Australian Citizens Party.

ASPI leads online censorship campaign

Numerous independent media publications have exposed social media companies' willingness to act as a censorship arm of the US government. Documents leaked in 2013 by whistleblower Edward Snowden, a former contractor to the CIA and US National Security Agency (NSA), revealed that "Five Eyes" (USA, UK, Australia, Canada and New Zealand) intelligence agencies worked closely with Big Tech to conduct mass internet surveillance. ASPI, which received funding from social media giants Facebook, Twitter and Google, has functioned as a key player in this global censorship fraternity, which involves powerful think tanks, Big Tech, and intelligence-connected organisations. This censorship network cooperates to create and drive allegations that foreign governments, particularly China and Russia, are conducting cyber-influence operations through social media.

Since 2018, Twitter has periodically announced mass purges of accounts which have been deemed "state-linked information operations", which Twitter primarily attributes to China and Russia. However, in official testimony Twitter has appeared to hedge its bets, calling them "potentially" or "suspected" state-backed information operations.[2] Nevertheless, ASPI has repeatedly relied on Twitter's announcements as evidence that the Chinese government is the architect of Spamouflage.

ASPI has enjoyed a privileged position as one of three select "research partners" to receive early and exclusive access to Twitter's "state-linked" bot account datasets. ASPI works closely with Twitter to apply "analytic and *narrative* context" to Twitter's datasets (emphasis added). Although at times ASPI has admitted that it did not have access to Twitter's raw data to verify independently that bot accounts were actually linked to the Chinese government, ASPI's analysis, which has been paid for by Twitter (see Box), has supported Twitter's decisions to permanently remove hundreds of thousands of accounts which have been attributed to Chinese "state-linked operations". Another of Twitter's partners is Graphika collaborator and research partner the Stanford Internet Observatory (SIO). SIO is headed by Alex Stamos, an advisory board member of NATO's Collective Cyber Defence Centre of Excellence, who joined Stanford from his role as Chief Security Officer at Facebook. In April 2023, representatives of SIO were guest speakers at ASPI's invitation-only Sydney Dialogue, which was sponsored by Meta, Facebook's parent company.

Participants in this global censorship operation have done exactly that which they accuse the Chinese government of doing. For example, as reported by investigative journalism website The Grayzone on 2 November 2021, one week before the November 2021 Nicaraguan elections, social media giants Facebook, Twitter, YouTube (Google) and Instagram launched a massive censorship sweep of social media accounts, including those of media outlets, journalists and activists, which supported the left-wing Sandinista government. Facebook refused to distinguish between real people and alleged spam accounts, justifying mass account deletions by claiming that all were state-backed bots. Nicaragua has previously been subject to US government-sponsored destabilisation efforts, including a violent attempted *coup d'état* in 2018.

[1] "'Longer Telegram' a recipe for war with China", *AAS*, 10 Feb. 2021.

[2] Twitter's submission to the Australian Foreign Interference through Social Media Inquiry, April 2020; Twitter's testimony to US House of Representatives Committee on Homeland Security, 26 June 2019.

Similarly, Graphika played a key role in the coordinated government-media-intelligence operation to destroy the election campaign of UK Labour Party leader Jeremy Corbyn. When Corbyn made damaging revelations about his opponents' intent to sell off Britain's national healthcare system to foreign interests, Graphika swiftly produced highly publicised "research", led by Ben Nimmo, which suggested that Corbyn's documents were part of a Kremlin disinformation campaign. Graphika's allegations allowed the media to deflect attention from Corbyn's revelations, by smearing him as a vehicle for a supposed Russian disinformation operation.

The big question

Since 2019, sensationalised reporting of Spamouflage has supposedly "outed" China as the culprit of this covert cyber-interference campaign. Because of this, any other bot campaigns which can be linked (however tenuously) with Spamouflage, such as ASPI's supposed Australia-targeting bot network, can also be conveniently blamed on the Chinese government. However, Spamouflage's attribution should be taken with a grain of salt, as it invariably comes from organisations which have proven aligned with the interests of the US government; are closely connected to intelligence agencies; or are associated with Anglo-American propaganda operations, such as the Integrity Initiative.

Despite China's alleged authorship of Spamouflage, social media companies consistently acknowledge that Spamouflage has very low-quality content and virtually zero organic engagement or reach, meaning that it is totally ineffective as propaganda. Why would the Chinese government persist in conducting such an ineffective and politically damaging foreign influence operation?

Although totally ineffective as a Chinese government propaganda campaign, Spamouflage and its associated bot networks *are* a highly useful Five Eyes propaganda tool. Sensationally hyping so-called "state-linked information operations" provides valuable media fodder and justifies mass purges of accounts, in which genuine users with undesirable views can be deleted along with alleged state-backed bots. It also provides "evidence" to push for policy change—for example, the hearings of Australia's recent parliamentary Inquiry into Foreign Interference through Social Media have been stacked with ASPI associates. The alleged threat of Spamouflage also allows for guilt-by-association attacks—such as ASPI's claim that the Chinese government is covertly promoting the Australian Citizens Party's social media accounts. It is evident that the primary beneficiary of the Spamouflage network is not the Chinese government; it is the US government and its Five Eyes allies.

The US government is certainly capable of conducting a "false flag" social media bot campaign to be blamed on the Chinese government. On 17 March 2011, the *Guardian* revealed that the US military had contracted a private company, which was headed by a thirty-year veteran of the CIA, to develop sophisticated software that would let the US military "secretly manipulate social media sites by using fake online personas to influence internet conversations and spread pro-American propaganda". These inauthentic "sock puppet" accounts could appear to be based anywhere in the world. It is not far-fetched to consider that this software could be repurposed for other social media manipulation campaigns. Hence the obvious question: Is the US State Department funding ASPI to produce reports on so-called Chinese cyber-influence bots, which are actually a tool of the US government?

ASPI's funding reveals role as foreign influence conduit

The Australian Strategic Policy Institute presents itself as an "independent, non-partisan" policy think tank, despite evidence of its overwhelming bias towards the geopolitical interests of the United States and other Five Eyes nations. ASPI has been the primary agitator in Australia against the Chinese government, and is leading the insane drive to war. ASPI's funding sources, however, prove that its so-called "independence" is a farce.

The majority of ASPI's funding comes from the Australian federal government, but ASPI also receives funds from foreign governments, the private sector, and the arms industry. In 2021-22 15.6 per cent ($1,939,442) of ASPI's total funding was sourced from foreign governments, including Five Eyes nations the United States, United Kingdom, and Canada; and the governments of Japan and the Netherlands. A whopping 76 per cent ($1,483,760) of ASPI's foreign government funding in 2021-22 was provided by the United States, dwarfing its next-largest contributor the UK, at 15 per cent ($296,862).

Notably, ASPI's "sources of revenue" graph in its annual report of the previous year (2020-21) did not include a $5 million payment from the US government to establish ASPI's Washington DC branch over the next two years. Instead, this funding was recorded separately to ASPI's overall sources of revenue, because ASPI claimed it would "create a mismatch between income and expenses in the next two financial years".

In 2021-22, 10.7 per cent ($1,339,990) of ASPI's funding was sourced from the private sector. This included $500,000 from Meta (Facebook) to sponsor ASPI's 2023 invitation-only Sydney Dialogue, and an additional $135,000 for "corporate sponsorship". ASPI received $99,656 from Twitter for "disinformation/takedown data analysis works support", which evidently refers to ASPI's help in facilitating Twitter's mass purging of alleged state-backed "inauthentic" accounts. Google contributed $70,000 to ASPI in 2021-22. In addition to funding contributed in 2021-22, ASPI has received significant funding from social media giants Google, Facebook, and Twitter over the last four years, which coincided with ASPI's escalating allegations that the Chinese government is conducting cyber-influence campaigns through social media.

Unsurprisingly, as ASPI functions as Australia's war-propagandists-in-chief, ASPI also receives funding from the world's largest arms manufacturers and has deep ties to the defence industry. In 2021-22, 3.3 per cent ($410,182) of ASPI's funding came from "defence industries", including weapons manufacturers Boeing, Lockheed Martin, Omni, Saab and Thales. A 1 April 2021 article by Marcus Rubenstein for *APAC News* documented that, since its founding in 2001, ASPI's defence industry sponsors have raked in over $51 billion in Australian government contracts. Rubenstein documented that 49 of ASPI's other sponsors, who do not manufacture weapons, have benefited from over $30 billion in Australian defence contracts. A 20 January 2022 investigation by online publication MintPress News revealed that many of ASPI's senior council members have had deep connections with the arms industry, including serving in executive positions on the boards of large weapons manufacturers.

ASPI's 'cyber-interference' allegations: more junk research

By Melissa Harrison

Canberra's chief warmonger, the Australian Strategic Policy Institute (ASPI), is hell-bent on driving Australia into conflict with our largest trading partner, China. For several years ASPI has repeatedly accused the Chinese government of conducting foreign interference operations against Australia. ASPI's dubious "research", however, has been consistently debunked and discredited by the Australian Citizens Party and other researchers. The latest iteration of ASPI's Chinese influence hysteria is "cyber-enabled foreign interference", or "state-backed information operations", which are ostensibly conducted through social media platforms.

Cyber-enabled election interference

ASPI alleges that foreign governments—invariably those targeted by Anglo-American strategic agendas—have used social media to interfere in (primarily Western) elections. However, ASPI's allegations are overwhelmingly sourced to Western mainstream media publications and think tanks, and intelligence-connected organisations.

In a 2019 report, *Hacking democracies; Cataloguing cyber-enabled attacks on elections*, ASPI claimed that China and Russia were the main perpetrators of cyber-enabled foreign interference in elections in 20 countries between 2016 and 2019. ASPI's analysis was based on incidents which were publicly reported by sources such as mainstream media; US government-funded propaganda organ Voice of America; NATO-affiliated think tank the Atlantic Council; and intelligence-connected cybersecurity company FireEye. *Hacking democracies* was produced with funding from the Australian Computer Society (ACS), the representative body for the information and communications technology sector, and included a foreword authored by ACS president Yohan Ramasundara. ASPI did not disclose that Ramasundara also worked for the Australian government, as Director of Business Futures at IP Australia.

One of ASPI's examples of election interference included mainstream media claims that in 2017, persecuted Australian journalist and WikiLeaks founder Julian Assange had acted as the "principal international agitator" in the lead-up to the Catalan independence referendum, because Assange criticised the Spanish government on Twitter. ASPI wrote that Assange was "promoted and amplified by Russian state-sponsored media outlets and Twitter bots". The charges against Assange were levelled by the Atlantic Council's Ben Nimmo, a key participant in a global censorship operation involving Big Tech and intelligence-connected organisations, which accuses the Chinese and Russian governments of foreign interference through social media. ("ASPI central in global censorship network", *AAS*, 9 Aug. 2023.)

ASPI relied on hearsay to claim that Australia had been the target of election interference. On 18 February 2019 Prime Minister Scott Morrison sensationally announced that hackers had targeted Australian political parties. Despite acknowledging that the Australian government had not specified which state was responsible for the alleged operation, *Hacking Democracies* attributed the attack to China, because "many commentators had publicly identified China as the most likely" culprit.

Questions over ASPI's methodology

In March 2022 ASPI launched the US State Department-funded "Understanding Global Disinformation and Information Operations" website, which displayed interactive visual representations of alleged "state-linked information operations" conducted on Twitter. The website used datasets provided by Twitter, with "context of geopolitical tensions" added by ASPI. Anglo-American geopolitical targets Russia, Iran, China and Venezuela, along with Saudia Arabia, were alleged to be the most prolific perpetrators of cyber-enabled foreign interference. However, although ASPI admitted that much of the data was "spam" or commercial content, ASPI's methodology did not adequately filter out commercial tweets that ran concurrently to the alleged influence operations, making it "difficult to identify and assess the most significant content shared in the datasets", which comprised hundreds of millions of Tweets. There are questions over whether these were actually state-backed information operations, as ASPI and Twitter claimed. In the example of China, the top ten most-shared links of these alleged Chinese government cyber-interference operations included a British hamper company; "Happy Muslim Family", a relationship advice website; and numerous defunct websites and broken links.

ASPI works closely with Twitter to provide analysis to support Twitter's mass purges of accounts deemed Chinese state-backed information operations, and has received funding from Twitter for this work. However, ASPI has admitted that it did not have access to Twitter's relevant data to verify independently whether accounts actually were linked to the Chinese government.

Poor evidentiary standards

ASPI's evidentiary standards for attributing social media "bot" activity to the Chinese government are very low. Its 24 July 2023 article titled "China's cyber interference narrows in on Australian politics and policy" is a typical example. ASPI analysts alleged that Chinese state-backed social media "bots"—automated software which engages on social media, usually using fake accounts which mimic real people—were interfering in Australia's domestic and foreign policies. ASPI claimed these bots criticised Australian spy agencies, AUKUS, the US-Australian alliance, and ASPI itself; and promoted the views of "certain individuals", naming former Prime Minister Paul Keating and the Australian Citizens Party (ACP), who are outspoken critics of ASPI's warmongering against China.

Conspicuously missing from ASPI's analysis is a curious phenomenon: the majority of these so-called Chinese government bots, which comment on Twitter posts of the ACP and its members, have *also* posted spammy content lauding US Republican Senator Marco Rubio. Rubio is a well-known agitator *against* the Chinese government. Why would Chinese state-backed bots promote China-basher Marco Rubio?

The basis for ASPI's claim that these bots were part of a Chinese government operation came down to ASPI's assessment that they displayed "behavioural traits" which linked them to "Spamouflage", a larger spam network which social media companies and various intelligence-connected organisations have attributed to the Chinese government.

ASPI claimed that this supposed Chinese state-backed bot network was linked to "transnational criminal organisations", suggesting that the Chinese government was now utilising organised crime networks to conduct its cyber-influence operations. However, this sensational allegation was based solely on ASPI's assessment that the Australia-targeting bot network was connected to another spam network which promoted the Warner International Casino. ASPI described Warner casino as "an illegal online gambling platform operating out of Southeast Asia and linked to Chinese transnational criminal organisations".

ASPI claimed that the Australia-targeting bots and the Warner Casino bot networks were connected because the accounts had similar stock photos or used AI-generated images as profile pictures; or tweeted the same nonsensical comments, or phrases which were typically cut off mid-sentence. ASPI also claimed that the Warner-promoting bots posted "CCP propaganda"; however the only example ASPI provided was a single half-sentence tweet, which stated: "The Third Plenary Session of The sixteenth Central Committee clearly developed people-oriented, comprehensive, coordinated and sustainable d—". An internet search shows that, like other Warner bot posts, this so-called "CCP propaganda" was just a phrase scraped from online content, from the now-defunct China Geological Survey website. ASPI claimed that four Warner-promoting bots were also linked to "CCP covert influence operations targeting Australia", however the only content these accounts have published was related to nuclear waste dumping from Japan's Fukushima disaster. Despite the paucity of evidence, ASPI's claim that so-called Chinese government bot accounts were linked to international criminal syndicates was promoted by Australian mainstream media.

'Operation Honey Badger'

ASPI's April 2023 policy brief, the US State Department-funded *Gaming Public Opinion*, typifies ASPI's questionable standards of analysis. *Gaming Public Opinion,* which alleges that the Chinese government conducts global "covert cyber-enabled influence operations", was peer reviewed by ASPI staff and anonymous "external reviewers from industry and government" (ASPI does not specify which government). ASPI loftily claimed that "only a few research teams globally have the capability and right mix of language, analytical, technical and data skill sets" to analyse cyber-influence datasets disclosed by social media platforms. ASPI named itself, intelligence-connected cyber-analytics firm Graphika, and Graphika's research partner the Stanford Internet Observatory, as three organisations which possessed this capability. These organisations have worked closely with Big Tech companies to purge hundreds of thousands of social media accounts on the basis that they were deemed "state-linked information operations", although investigative reporting has identified that genuine users with views undesirable to the Anglo-American establishment have been deleted along with alleged state-backed bots.

Gaming public opinion

The CCP's increasingly sophisticated cyber-enabled influence operations

Albert Zhang

With Tilla Hoja and Jasmine Latimore

INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 71/2023

In *Gaming Public Opinion*, ASPI presented a case study of an alleged Chinese government "cyber-enabled influence operation", which ASPI claimed was a new iteration of the so-called Spamouflage bot network. The authors of *Gaming Public Opinion* sensationally announced that they believed it was "possible" that Chinese government agencies had named this propaganda campaign "Operation Honey Badger". However, the only evidence provided to support this was a Tweet posted by an account which ASPI claimed was "likely to be affiliated with the CCP", which showed a screenshot of a computer desktop that displayed a Chinese-language version of the text of an alleged Spamouflage-associated blog post (which could have been copied and pasted from anywhere). An additional browser tab, of which the contents are hidden, was titled "Operation Honey Badger". Despite this ludicrously flimsy "evidence", ASPI devoted considerable effort to ruminating over the possible motivation of the alleged name—"it's unclear why this operation was named Operation Honey Badger but there a few plausible explanations. One reason could be that honey badgers are known for fighting larger predators in Africa, southwest Asia and the Indian subcontinent. In this operation, the honey badger might be representing the PRC fighting the hegemony of the US which is symbolised as a larger predator. Operation Honey Badger could also possibly be a reference to a CIA and Federal Bureau of Investigation operation to find Chinese moles and investigate why Chinese informants were disappearing in 2010".

ASPI claimed that this new Spamouflage spin-off promoted the narrative that US government intelligence agencies had conducted cyber operations against China, and portrayed China "as a victim of false hacking accusations". As ASPI observed, the artistic style and imagery of "Operation Honey Badger" was similar to previous bot campaigns which ASPI has linked to Spamouflage. In all of these supposed Chinese state-backed campaigns, the imagery used is of very poor quality, and includes misplaced text and poorly edited screenshots. The juvenile and crude cartoons are extremely off-putting and invoke a negative reaction towards the poster, rather than any sympathy for the message—hardly the desired outcome for a supposed propaganda campaign with the resources of the Chinese government behind it.

ASPI assessed that Operation Honey Badger accounts were part of the alleged Chinese government operated-Spamouflage network because the accounts "share the same characteristics", including "the use of Western female personas" and AI-generated profile pictures, and because they shared the same links. ASPI also noted that Operation Honey Badger posts were "mostly published during the Beijing time-zone work week and business hours", omitting the inconvenient fact that numerous other countries share the same time zone as Beijing, as does Western Australia. ASPI claimed that the operation was also active on Chinese social media sites, "confidently" linking 200 accounts to Spamouflage because those accounts shared the same images and "rarely had original profile images and instead used either default images, cartoons or pictures of female models, all of which Spamouflage-linked accounts on Western platforms often used."

ASPI claimed that "some evidence suggests" that Operation Honey Badger accounts were "possibly affiliated" with the Yancheng (Jiangsu province) Public Security Bureau, a provincial government policing organisation, and the Chinese government's Ministry of Public Security (MPS). However, there are serious questions over the reliability of ASPI's "evidence".

ASPI claimed to have geolocated Operation Honey Badger posters to Jiangsu, where the Yancheng Public Security Bureau is located. However, ASPI's analysis relied upon the "social listening services" of Norwegian software company Meltwater, which can only "infer" geolocation based on information which the poster publicly provides. Additional "evidence" ASPI provided to link Operation Honey Badger to Chinese policing and security organisations, was that several fake accounts only followed the social media accounts of the official Traffic Police Detachment of Yancheng Public Security Bureau; the MPS; or "New Police Matters", which is published in a government newspaper. ASPI's "evidence" also included two Weibo (Chinese social media platform) accounts, one of which appeared to have a "selfie" of a Chinese police officer as its profile picture, and another account which used a Jiangsu police station as a profile image.

ASPI claimed that while police officers "were likely involved in coordinating Spamouflage propaganda campaigns", the operation of most fake accounts was "possibly" outsourced to a "specially trained—and ideologically sound—group of ‘internet commentators’” employed by Chinese government agencies. An example of ASPI’s dubious standards of analysis can be seen in the think tank’s profiling of an alleged Spamouflage-linked account, which was supposedly operated by one such hired internet commentator. ASPI hypothesised that this Yancheng-based account was “most likely operated by a young male”, because the user had bookmarked posts “warning men not to take their girlfriends travelling unless their relationship is strong enough or they’ll break up” and “‘common sense’ facts about women that men might not know”. Without evidence, ASPI theorised that he was probably a part-time student living in Yancheng. Because the user had previously bookmarked articles about registering for self-study examinations in Jiangsu, ASPI asserted he was “unlikely to be a public servant because it’s generally difficult for students without a university degree to get those jobs”. It is difficult to understand how ASPI considered such meaningless hypothesising to be worthy of inclusion in a US government-funded report.

Ultimately, ASPI admitted its “analysis” did not prove anything: “To be clear: while we unearthed potential links, we didn’t find sufficient publicly available evidence to say with full confidence that Yancheng Public Security Bureau or MPS-affiliated individuals are directly operating Spamouflage accounts.”

Labor’s ‘renewables are cheapest’ lie exploded

By Richard Bardon

Prime Minister Anthony Albanese and Energy Minister Chris Bowen’s mantra that “firmed renewables” are the cheapest pathway to a so-called net-zero greenhouse gas economy, and that the alternative zero-emissions technology, nuclear, is the most expensive, is based upon blatantly deceptive modelling that hides the overall costs of the former and exaggerates those of the latter. Independent analysis by physicist and data analyst Aidan Morrison shows that the annual “GenCost” report produced by national science agency the Commonwealth Scientific and Industrial Research Organisation’s (CSIRO) and gas and electricity systems overseer the Australian Energy Market Operator (AEMO), to which Bowen habitually refers as proof that “renewables” are cheapest *at present*, in fact projects that they will *eventually become cheapest after 2030*; and it does so by writing off the enormous upfront expense of all the major projects which must be completed before then as “sunk costs”. For current “full system costs”, the CSIRO passes the buck to the AEMO’s Integrated System Plan (ISP). That report, however, does not properly account for the full cost of renewables either, and does not examine the costs of nuclear at all. It would seem that in energy as in so many other policy areas, at best Labor is simply not up to the job, and at worst is deliberately deceiving the Australian public.

The 24 January *Australian Financial Review* reported that in response to criticism from nuclear advocates that he and Albanese were “hiding behind the cost argument” to conceal their ideological opposition to nuclear power, “Mr Bowen said the latest CSIRO GenCost report showed nuclear energy was by far the most expensive form of energy in Australia. ‘Even if Australia started working on a nuclear energy industry now, it wouldn’t be operational by the end of the decade, with nothing to help reduce energy costs for Australian households and businesses in the meantime’, he said. ‘The same GenCost report shows *firmed renewables, with transmission and storage, are the cheapest form of energy*, and getting cheaper every day. That’s why the Albanese government has made huge investments in renewable energy, like Marinus Link in Tasmania and VNI West Link in Victoria. These projects will open up Australia’s renewable energy capacity … while putting downward pressure on power prices.’” (Emphasis added.)

There is no ambiguity here: Firmed renewables, *with transmission and storage*, “are” the cheapest, Bowen says. In the present tense, meaning now, today. But not only does the 2022-23 GenCost report say no such thing, in fact it explicitly *excludes* the costs of all “transmission and storage” infrastructure that has yet been built, or will be in the next 17 years. As the report’s lead author, CSIRO Chief Energy Economist Paul Graham, acknowledged in a 29 July letter to the editor of the *Australian* newspaper: “LCOE [the levelised cost of electricity] is a simple metric [used in the report] for non-modellers to understand the relative costs of energy from different generation technologies. The method essentially calculates the cost per MWh [megawatt-hour] that would have to be recovered for a new electricity generation investment to break even *if it were to take place in a given year such as 2030. The report does not provide the cumulative cost of all investments up to 2030*…. All existing generation, storage and transmission capacity up to 2030 is treated as sunk costs since they are not relevant to new-build costs in that year.” (Emphasis added.)

Again, there is no ambiguity here. If Bowen is not simply lying outright, then he has either not read, or perhaps has read but not understood, the report on whose basis he peddles falsehoods to the people of Australia.

Designed to deceive?

Arguing in favour of the latter, is that the GenCost report seems tailored to bamboozle. In its executive summary—mayhap the only part of such a document that Bowen would bother to read, however crucial a complete understanding of its subject matter might be to his portfolio responsibilities—the report states that “The LCOE is estimated on a common basis for all technologies. However, an additional process is undertaken to calculate the integration costs of variable renewables. The required amount of additional investment depends on the amount or share of variable renewable energy (VRE) generated. … When added to variable renewable generation costs and compared to other technology options, these estimates indicate that onshore wind and solar PV remain the lowest cost new-build technologies.” The blunt admission that all investments that have been and will be needed up to 2030 have been dismissed as “sunk costs” and not factored in, however, is buried in a footnote on the 85th of the report’s 97 pages.

What makes this so misleading, Aidan Morrison explains in an analysis published 23 July at economist Dr Cameron Murray’s “Fresh Economic Thinking” blog, is that integration costs per MWh of renewables over the course of the “transition” are nowhere near as constant or uniform as the GenCost report seemingly seeks to imply. “The supporting infrastructure comes in big, lumpy projects, highly specific to the geography and meteorology of a grid”, Morrison wrote. And by 2030, by which time we are supposed to have surpassed 50 per cent renewables, almost all such projects will need already to have been built. “We can see this on page 52 of the report, which describes their ‘Business As Usual’ scenario, i.e. all the projects which are specifically *excluded* from the incremental costs of integrating new solar and wind”, Morrison noted (emphasis in original). “It’s packed full of

Continued page 9