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

Fergus Ryan is a Senior Analyst and Albert Zhang is an Analyst at the Australian Strategic Policy Institute. Emily Mosley, a Program and Research Coordinator within ASPI's International Cyber Policy Centre, contributed and helped coordinate this submission. We research disinformation and the deliberate manipulation of the information environment to achieve strategic goals—what we will refer to here as influence operations. The views expressed here are our personal opinions as ASPI does not take corporate positions on any issues.

Introduction

Social media platforms are now contested spaces for malign actors to achieve their strategic, economic or political goals. Authoritarian governments seek to silence their critics, weaken democratic institutions and shape international narratives to favour their interests, while non-state actors exploit unmediated access to Australians to profit or pursue ideological aims. To a large extent, Western governments have chosen to leave the development of social media to the private sector, convinced (including by the private sector) that government involvement would stifle innovation. A lack of standards, rules and enforcement measures, however, has resulted in cyber-enabled foreign interference impeding the independent decision-making of the public, businesses and policy-makers. While the internet has increased our access to valuable information, it has also increased the spread of disinformation and imposed costs on Australians to freely express their opinions.

Many state and non-state actors use social media for public diplomacy and propaganda but this submission focuses on foreign interference and influence operations through social media that are covert, corrupting and coercive. There are also many different state and non-state actors engaged in such activity, and this submission will touch on a range but will focus on the Chinese Communist Party (CCP) given it is the key actor in the Indo-Pacific engaging in the widespread promotion of disinformation and cyber-enabled foreign interference. It is also engaging directly, and currently, in malicious activity in Australia, including efforts to interfere in political discourse and targeting Australian politicians.

Over the past few years, Australia's strategic circumstances have grown more challenging and destabilised the way information is shared and consumed online. The Covid-19 pandemic saw health and vaccine misinformation grow rampant, partly due to increased stresses, and partly stoked by fearmongering by state and non-state actors alike.[1] In 2022, Russia's depiction of its further invasion of

[1] Jarrod Lucas. 'WA Premier Mark McGowan says US white supremacists are targeting remote communities', *ABC Goldfields,* 3 Dec 2021. online.

Ukraine as a 'special military operation' and joint claims with the CCP of US bioweapon laboratories,[2] reminded all of us that online disinformation and propaganda are key aspects of modern conflict.

Our understanding of foreign interference through social media has improved since Russian meddling in the 2016 US election but much work remains to be done. ASPI's analysis of publicly available Twitter data from state-linked information operations shows that at least 17 countries globally are exploiting social media as a vector to covertly influence their domestic and international audiences.[3] In particular, Beijing, Moscow and other regimes are using social media to control their domestic populations by censoring and setting agendas and are also competing for control of international narratives by disseminating disinformation and sowing discord. As our ASPI colleagues wrote in their 2020 submission to the Select Committee on Foreign Interference through Social Media, online influence operations, however, are not limited to nation-states or to just election periods.[4]

The lack of effective denial and deterrence has allowed these activities to occur more frequently and become more sophisticated. Countermeasures need to shift from reactive responses to proactive ones rapidly. Once social media is used to spread disinformation or for interference, it is difficult to rein in. Our key recommendations for the Australian government are, with further details provided below:

1. The Australian Government should implement more rigorous data privacy and data protection legislation.
2. The Australian Government should incorporate countering cyber-enabled foreign interference into cybersecurity and national security strategies.
3. The Australian Government should consider mandating platforms to disclose cyber-enabled foreign interference activity.
4. The Australian Government should provide more specific definitions surrounding ambiguous terms in the DIGI Code.
5. The Australian Government should make public diplomacy and deterrence core aspects of countering foreign interference through social media.
6. Law enforcement should work with social media platforms to increase public awareness of transnational repression.

Foreign interference through social media

Cyber-enabled foreign interference now includes a range of information manipulation activities across multiple social media platforms including US-based ones, such as Twitter, Facebook, Instagram, Reddit or YouTube, and Chinese-originated ones, such as TikTok, WeChat and Weibo. In this contested information environment, we believe there are three areas that the Australian government should

[2] Samantha Hoffman, Matthew Knight. 'China's messaging on the Ukraine conflict', *ASPI*, 23 May 2022. online.
[3] Jacob Wallis, Albert Zhang. 'Understanding Global Disinformation and Information Operations: Insights from ASPI's new analytic website', *ASPI,* 30 March 2022. online.
[4] Jacob Wallis, Thomas Uren. 'Submission to the Senate Select Committee on Foreign Interference through Social Media', *Parliamentary Committee on Foreign Interference through Social Media Submissions,* 2020. online.

prioritise to secure our values and interests: (1) transnational repression in Australia, (2) efforts to undermine public trust in democratic institutions, and (3) efforts to manipulate international markets.

Transnational repression

Well-resourced state and non-state actors are using social media platforms to facilitate the transnational repression of individuals and marginalised communities in Australia. This poses a significant threat to the freedom of Australians, and others residing in Australia, to express their opinion and access online spaces. According to Freedom House, transnational repression is when 'governments reach across national borders to silence dissent among their diaspora and exile communities'.[5] On social media, this includes online trolling, stalking or harassment, and is typically conducted by authoritarian states to coerce their citizens and others abroad.

ASPI research has shown that the Chinese Communist Party (CCP) is targeting women of Asian descent and subjecting them to high levels of personal abuse in an effort to counter their views and discredit their work.[6] An example of this is the campaign targeting ASPI senior fellow Vicky Xu by a network of inauthentic Twitter accounts we believe is affiliated with the CCP and which has previously been confirmed by Twitter.[7] This network often accused Xu, and other women, of being traitors and liars but also used graphic online depictions of sexual assault, homophobia and racist imagery (sometimes involving Australian lawmakers) and life-threatening intimidation (including calling for targets to kill themselves).[8] This activity appeared to be coordinated with a broader public propaganda campaign by the Chinese government to silence women of Asian descent who have criticised its policies.[9]

Transnational repression is not unique to the CCP and appears to be a common tactic deployed by other authoritarian regimes in our region. The Iranian government has reportedly been monitoring the online presence of people attending protests in Australia against the Iranian government's policies.[10] Pro-regime accounts have also subjected Australians to extensive harassment and bullying online due to their criticism of the Iranian morality police. Senator Penny Wong has released statements regarding the threats online, stating the harassment of Australian protesters and their families in Iran has been reported to the Department of Home Affairs, and that foreign interference will be investigated and prosecuted if necessary.[11]

---

[5] Nate Schenkkan, Isabel Linzer. 'Out of Sight, Not Out of Reach', *Freedom House.* Feb 2021. online.
[6] Albert Zhang, Danielle Cave. 'Smart Asian women are the new targets of CCP global online repression', *ASPI The Strategist*, *3 Jun 2022. online.*
[7] Bethany Allen-Ebrahimian, 'Report: China-linked Twitter harassment targets female Asian journalists outside China', *Axios,* 3 Jun 2022, online; Adam Rawnsley, 'Why Is Twitter Shutting Down Chinese Activists' Accounts?', *Rolling Stone*, 9 December 2022, online.
[8] https://web.archive.org/web/20221024054748/https:/twitter.com/Johni7Chruchiil
[9] Zeyi Yang, 'The anatomy of a Chinese online hate campaign', *Protocol*, 9 April 2021, online.
[10] Josh Butler, 'AFP urges Iranians in Australia to report harassment by Tehran authorities as anti-government protests escalate', *The Guardian*, 21 December 2022, online.
[11] https://twitter.com/SenatorWong/status/1594937398818914305?s=20&t=gq6hRtsGVBqBLgTNX61Hww

Likewise, the Centre for Information Resilience has analysed Telegram posts abusing women in, and from, Myanmar who opposed the military coup and found some evidence of coordination between online abusers and Myanmar security forces.[12]

This online repression is happening largely without consequence partly because there is uncertainty as to which agency in Australia has responsibility. Often victims are pushed from intelligence agency to intelligence agency or from intelligence agency to law enforcement agency and from Commonwealth to State jurisdiction. This lack of responsibility means there will be a lack of disincentives for perpetrators to cease their activity and a lack of incentives for victims to persist in seeking justice.

Undermining public trust in democratic institutions and leaders

Foreign state actors are exploiting social media to interfere directly in the democratic processes of Australia and fostering distrust of its leaders and political institutions.

ASPI research on the CCP-affiliated network trolling and harassing women uncovered a sophisticated subnetwork promoting fringe Australian political parties and individuals supportive of pro-CCP foreign policies.[13] Most of these accounts were suspended after the publication of our report but we have since discovered that the network has replenished its assets and escalated its efforts to interfere in Australian online political discourse.

For this submission, ASPI identified at least an additional 33 inauthentic accounts very likely linked to this CCP-affiliated network, which is promoting negative news content about Australian politicians, in English and Mandarin, and using the hashtags #Auspol and #QandA, two of Australia's most popular hashtags for discussing domestic politics. For example, multiple accounts are using fake Western personas to artificially amplify stories about an allegation that former Attorney-General Christian Porter raped a woman in 1988, in an effort to make this topic trend for Australian social media users. Other posts call for societal and cultural changes in response to 'sex scandals' in the Australian Parliament and some posts fabricate their own claims that have not previously been reported in Australian media or otherwise made publicly. The timeline of these accounts shows that they were also interfering in the 2022 US midterm elections by supporting Senator Marco Rubio. This campaign may have been connected to a pro-CCP campaign identified by Meta in September 2022, which was presumed to both support and undermine Republican candidates in a bid to sow division in the US.

Overall, the network is promoting criticism of politicians and policies of both Australian major parties, suggesting this campaign is seeking to undermine public trust in the Australian government and democratic system, rather than favouring any particular party. These accounts, however, lacked an in-depth understanding of Australian politics (posts would often incorrectly refer to 'congress' and the

[12] 'Digital Battlegrounds: Politically motivated abuse of Myanmar women online', *Centre for Information Resilience*, 27 January 2023, online.
[13] Danielle Cave and Albert Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women', *The Strategist*, 6 November 2022, online.

'Capitol') and appear to be copying and pasting other tweets by legitimate Twitter users. The content amplified in these campaigns was not always necessarily disinformation but the covert manner in which the accounts are artificially amplifying the reach of the reports interferes with the autonomy of Australians to make independent and informed views on the issues.

While the CCP is one major actor seeking to covertly influence political discourse in Australia, other malign actors are exploiting the reach and cost-effectiveness of social media campaigns. Earlier in 2022, a pro-Russian online commentator kicked off a harassment campaign against Ukraine's ambassador to Australia by posting his mobile phone number in a YouTube video, presumably to intimidate the ambassador and undermine his public support for Ukraine.[14] According to an ABC Article in February 2022, Australian intelligence has investigated at least one major case of Russian influence in the 2022 Federal election and believes Russian plots are still active.[15]

Non-state actors are also purchasing commercial services to interfere in elections and manipulate political discourse. ASPI research has explored this growing influence-for-hire industry and examined five case studies of online manipulation in the Philippines, Indonesia, Taiwan and Australia.[16] More recently, a special investigation by international journalists uncovered a team of Israeli contractors that offered disinformation on social media services and claimed to have manipulated public opinion across Africa, South and Central America, the US and Europe.[17]

Manipulating international markets

Foreign malign actors are conducting influence operations online to manipulate international markets and undermine Australian economic interests. These campaigns demonstrate that foreign interference with political motivations can negatively impact Australian, and regional, economic interests.

In 2022, ASPI uncovered a CCP-linked network of inauthentic social media accounts using environmental, political and health concerns to undermine efforts to diversify global rare-earth supply chains and support China's dominance of the industry.[18] A major target of the smear campaign was the Australian mining company Lynas Rare Earth and the Western Australian government. This campaign, along with other grey-zone operations, allowed the CCP to covertly impose costs on Australian

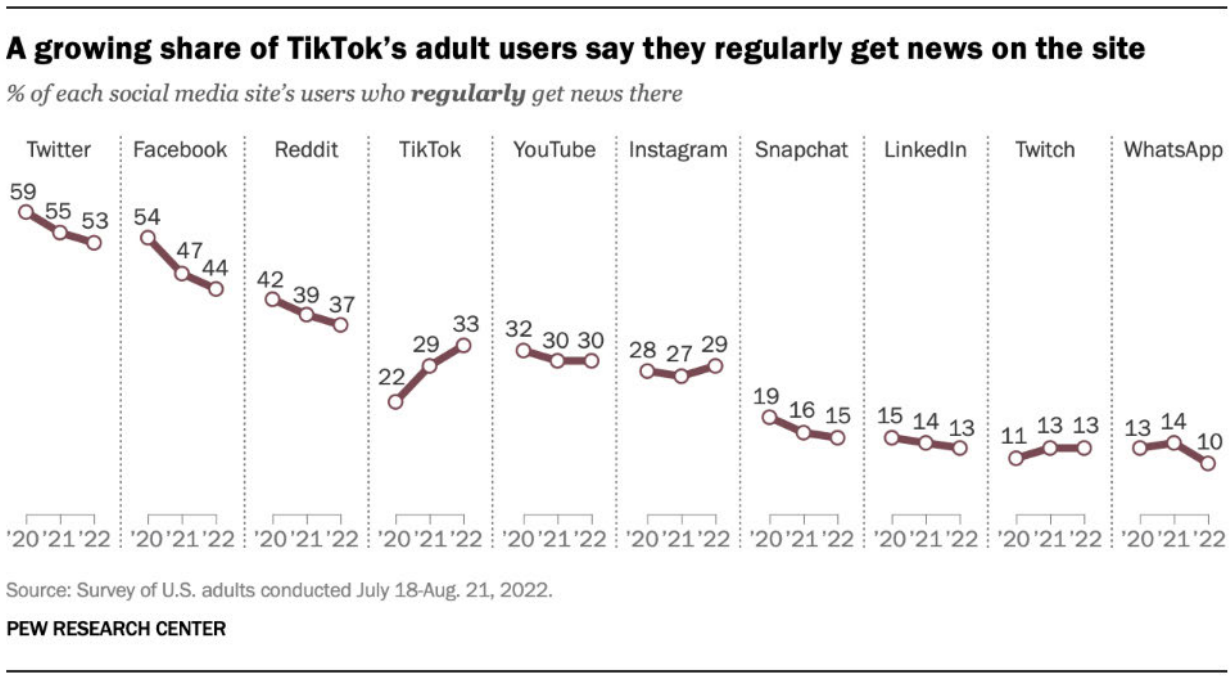
[14] Jessica Bahr and Tom Canetti, 'Australian YouTuber reported to police by Ukrainian ambassador over alleged 'harassment campaign,' *SBS News*, 7 January 2023, online.
[15] Andrew Greene, 'Intelligence officials identify Russian efforts to interfere in Australian politics,' *ABC News*, 10 February 2022, online.
[16] Jacob Wallis, Ariel Bogle, Albert Zhang and Hillary Mansour, 'Influence for hire. The Asia-Pacific's online shadow economy', *Australian Strategic Policy Institute*, 10 August 2021, online.
[17] Stephanie Kirchgaessner, Manisha Ganguly, David Pegg, Carole Cadwalladr and Jason Burke, ''Revealed: the hacking and disinformation team meddling in elections, *The Guardian*, 15 February 2023, online.
[18] Albert Zhang, 'The CCP's information campaign targeting rare earths and Australian company Lynas', The Strategist, 29 June 2022, online; 'Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance,' *Mandiant Threat Intelligence*, 28 June 2022, online.

companies with plausible deniability, preventing Australian companies and government officials from raising these actions with international bodies or directly with CCP representatives.

Covert activities on social media in support of economic interests are not a new tactic used by malign actors. Earlier in 2021, ASPI analysed a network of pro-Indonesian inauthentic social media accounts that challenged negative stories about Indonesia's palm oil industry.[19] The palm oil industry is a concern for Indonesia which, along with Malaysia, accounts for most of the commodity's global production. The inauthentic accounts identified in this network were coordinated, boosted Indonesia's Covid-19 vaccination campaign and displayed other behaviour suggestive of a Twitter network for hire.

Social media platforms and the broader information environment

The risks of foreign interference on social media are being exacerbated by the rapidly shifting news consumption habits of individuals in democracies and the declining public trust in Western social media platforms. According to Pew Research, more US adults say they are regularly getting news on TikTok while other social media platforms are seeing decreases in news consumption.[20] If this trend is similarly followed by Australians, then this has implications for the Australian Government's ability to regulate and cooperate with social media platforms that share fewer values in common - such as transparency - and may have less power to influence.



[19] See 'What's up with the BBC?': Jacob Wallis, Ariel Bogle, Albert Zhang and Hillary Mansour, 'Influence for hire. The Asia-Pacific's online shadow economy', *Australian Strategic Policy Institute*, 10 August 2021, online.
[20] Katerine Eva Matsa, 'More Americans are getting news on TikTok, bucking the trend on other social media sites', *Pew Research Center*, 21 October 2022, online.

Source: Pew Research Center.

Policymakers and legislators should ensure that when addressing the social media challenges (and broader technology risks) they do not disproportionately regulate Western technology platforms while ignoring technology platforms that originate from China or Russia. Democracies must not exacerbate the already unlevel playing field when our ultimate objective is to be able to compete against the authoritarian regimes which are abusing technology to further their strategic interests.

The Australian government must recognise that Moscow and Beijing's success in undermining democratic institutions is now being focused to undermine Western technology platforms at the advantage of authoritarian-originated technology platforms. This is happening before our very eyes without intervention and has been allowed to happen as Beijing and Moscow have taken a different approach to the rest of the world on social media. While the West thought the Arab Spring had demonstrated that social media was uncontrollable, Moscow and Beijing saw the threat and weaponised interference on social media to achieve their strategic purposes.[21]

Whether we like it or not, social media platforms now constitute one pillar of our nation's information ecosystem, which is broadly comprised of the individuals, organisations, technologies and relationships that contribute to the communication of information.[22] This includes influencers, TV broadcasters, news media organisations, websites, forums and social media platforms. This system forms a supply chain of information sharing that is critical infrastructure for the public to make informed decisions in a functioning democracy, akin to the criticality of the Australian electrical grid supplying power to people's homes.

For these reasons, the submission sets out below the risks posed by TikTok, which also extend to other social media platforms from authoritarian countries where appropriate.

TikTok

There are 3 main national security risks with the PRC-owned video-sharing app TikTok that Australians should be concerned about. Two of them—data and content manipulation—are applicable to most other major social media apps regardless of their country of origin. The third risk, that a single political party, the Chinese Communist Party has decisive leverage over TikTok, exacerbates the former two risks and is unique to TikTok as a major mainstream social media app.

The **first**, and most discussed risk is about data. Following years of scrutiny, TikTok has been forced to be more forthcoming about the fact that TikTok user data is accessible and has been accessed from the PRC. Close observers of TikTok statements from as early as 2020 know that it has only ever been

[21] Justin Bassi and Bec Shrimpton, 'Tech standard setting cannot be left to companies or lone nations', *Nikkei*, 9 February 2023, online.
[22] Thomas H. Davenport, 'Information ecology', *Oxford University Press*, 1997, online.

TikTok's *goal* for China-based employees to have *minimal* access to user data–not to cut it off completely.[23]

Furthermore, the app relies on this access to function. As stated in a September 2020 sworn affidavit by the company's then Chief Information Security Officer, 'TikTok relies on China-based ByteDance personnel for certain engineering functions that require them to access encrypted TikTok user data.'[24]

In 2023, this still has not changed. Even as the company puts into place its US$1.5 billion plan dubbed 'Project Texas' to move all data attached to American users to the United States, and to institute various governance, compliance and auditing systems to mitigate national security concerns, TikTok vice president Michael Beckerman maintains that engineers based in China "might need access to data for engineering functions that are specifically tied to their roles."[25] At a Senate hearing about social media and national security in September 2022, Vanessa Pappas TikTok's chief operating officer, declined to commit to cutting employees in China off from the app's user data.[26]

As long as PRC-based engineers are able to access TikTok user data, that data is at risk of being accessed and used by PRC intelligence services. TikTok's constant refrain that user data is stored in Singapore and the United States and that it would never hand over the data to the Chinese government even if it were asked is beside the point. The location in which any data is stored is immaterial if it can be readily accessed from China.

Moreover, TikTok's parent company, ByteDance, couldn't realistically refuse a request from the Chinese government for TikTok user data because a suite of national security laws effectively compels individuals and companies to participate in Chinese 'intelligence work'. If the authorities requested TikTok user data, the company would be required by law to assist the government and then would be legally prevented from speaking publicly about the matter.

Unfortunately, even if TikTok's parent company ByteDance were able to sever access to the app's user data from the PRC, Beijing's intelligence services could still readily access sensitive data on virtually anyone in Australia via the commercial data broker market.

Second, in what has unfortunately been an under-discussed risk, TikTok could continue to skew its video recommendations in line with the geopolitical goals of the Chinese Communist Party. This is a threat that continues to worsen as more and more people get their news and information from online platforms such as TikTok over which the Chinese party-state can control, curate and censor content.

---

[23] Roland Cloutier. 'Our approach to security', *TikTok Newsroom*, 29 April 2020, online.
[24] Roland Cloutier. 'Declaration of Roland Cloutier', *TikTok & ByteDance vs Donald Trump*, 23 September 2020, online.
[25] Michael Beckerman. 'Our approach to keeping U.S. data secure', *TikTok Newsroom*, 5 July 2022, online.
[26] David McCabe. 'Lawmakers Grill TikTok Executive About Ties to China', *The New York Times*, 14 September 2022, online.

There is ample evidence that TikTok has done this in the past. Leaked content moderation documents have previously revealed that TikTok has instructed "its moderators to censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong," among other censorship rules.[27] TikTok insists that those documents don't reflect its current policy and that it had since embraced a localised content moderation strategy tailored to each region.

In ASPI's 2020 report into TikTok and WeChat, we found they suppressed LGBTQ+ content in at least 8 languages.[28] After British MPs questioned TikTok executives about our findings, they publicly apologised.[29] Our report also included a deep dive on TikTok's Xinjiang hashtag & found a feed that was flooded with glossy propaganda videos with only 5.6% of those videos being critical of the crackdown on the Uyghurs.

In 2022, TikTok blocked an estimated 95% of content previously available to Russians, according to Tracking Exposed, a nonprofit organization in Europe that analyzes algorithms on social media.[30] In addition to this mass restriction of content, the organisation also uncovered a network of coordinated accounts that were using a loophole to post pro-war propaganda in Russia on the platform. In other words, at the outset of Putin's invasion of Ukraine, TikTok was effectively turned into a 24/7 propaganda channel for the Kremlin.

Following years of intense scrutiny, it is unlikely that TikTok will, in any overt way, become a conduit for pro-CCP propaganda. In a welcome sign in recent months, the company has even begun to label "China state-affiliated" accounts on the platform. It is unclear if these labels also ensure that the content is reduced on the platform as it currently does on other platforms like Twitter. To further build confidence, TikTok should, as other social media platforms have, regularly investigate and disclose information operations being conducted on the platform by state and non-state actors.

Any manipulation of the public political discourse on TikTok is likely to be subtle. Unfortunately, because each user's TikTok feed is different, any influence the CCP has over the app will be very difficult to track. It would be trivially easy for the app to, for example, promote or demote certain political speech in line with the CCP's preferences. The app could tip the scales in favour of speech attacking a political candidate who is critical of the CCP, for example.

TikTok certainly has the ability to detect political speech on the app as it monitors keywords in posts for content related to elections so that it can then attach links to its in-app elections center.[31]

---

[27] Alex Hern. 'Revealed: how TikTok censors videos that do not please Beijing', *The Guardian*, 25 September 2019, online.
[28] Fergus Ryan, Audrey Fritz & Daria Impiombato Impiombato. 'TikTok and WeChat Curating and controlling global information flows', *ASPI.* 8 September 2020, online.
[29] Umberto Bacchi. 'TikTok apologises for censoring LGBT+ content', *Reuters*, 23 September 2020, online.
[30] Salvatore Romano, Marc Faddoul, Claudio Agosti, Giulia Giorgi & Louise Doherty. 'TikTok blocks 95% of content for users in Russia', *Tracking Exposed.* online.
[31] Emily Baker-White. 'TikTok May Be Suppressing Videos About The Midterms And Voting, New Research Suggests', *Forbes.* online.

Experiments conducted by nonprofit group Accelerate Change found that including certain election-related words in TikTok videos decreased their distribution by 66%.[32] They also found that TikTok is consistently suppressing videos when it can detect they are about voting.

In 2020, U.S. TikTok executives noticed views for videos from certain creators about the U.S. presidential election were mysteriously dropping 30% to 40%, according to people familiar with the episode and cited by the Wall Street Journal. After making enquiries, the executives found out that a team in China had made changes to the algorithm to play down political conversations about the election.[33]

Algorithmic manipulation of content is not limited to TikTok. To take one recent example in February 2023, Twitter chief executive Elon Musk rallied a team of roughly 80 engineers to reconfigure the platform's algorithm so his tweets would be more widely viewed.[34] There is clearly a need for all social media companies to be more transparent about how changes to their algorithms affect the content users receive.

The **third** risk, rightly identified by Cybersecurity Minister Clare O'Neil as a "relatively new problem," is that apps like TikTok are, as the minister put it, "based in countries with a more authoritarian approach to the private sector."[35]

For TikTok's parent company ByteDance, this authoritarian approach has included compelling the company's founder Zhang Yiming to make an abject apology in a public letter for failing to respect the Chinese Communist Party's 'socialist core values' and for 'deviating from public opinion guidance'—one of the CCP's terms for censorship and propaganda.

The enormous leverage that the CCP has over the company is what drove the company at the time to boost its army of censors by an extra 4,000 people (candidates with party loyalty were preferred) and it's what continues to motivate ByteDance to conduct 'party-building' exercises inside the company.[36]

In April 2021, Beijing quietly formalised a greater role in overseeing ByteDance when state investors controlled by the China Internet Investment Fund (controlled by internet regulator CAC) and China Media Group (controlled by CCP's propaganda department) took a 1% stake in ByteDance's Chinese entity, Beijing ByteDance Technology, giving it veto rights over the company's decisions. At the time,

---

[32] Emily Baker-White. 'TikTok May Be Suppressing Videos About The Midterms And Voting, New Research Suggests', *Forbes.* online.
[33] Georgia Wells & Stu Woo. 'TikTok Tries to Win Allies in the U.S. With More Transparency', *Wall Street Journal*, 16 January 2023. online.
[34] Zoe Schiffer and Casey Newton. 'Yes, Elon Musk created a special system for showing you all his tweets first', *Platformer*, 15 February 2023, online.
[35] Anthony Galloway, 'Home Affairs to review data harvesting by TikTok and WeChat', *The Sydney Morning Herald,* 4 September 2022. online.
[36] David Bandurski. 'Tech Firms Tilt Toward the Party', *China Media Project,* 2 May 2018. online.

one of the other two seats on the company's board was held by Zhang Fuping (张辅评) who was the secretary of the company's Party Committee.[37]

More recently the CAC named a director from its bureau overseeing data security and algorithmic governance to the board of ByteDance's main Chinese entity. According to the Wall Street Journal, this director replaced another CAC official who was formerly part of the regulator's online opinion bureau.[38]

The PRC party-state is, in other words, completely intertwined with ByteDance to the extent that the company, like many other major Chinese tech companies, can scarcely be considered a purely private company that is only geared towards commercial ends. These companies are neither state-owned nor private, but hybrid entities that are effectively state-controlled.

Policy recommendations

Our key recommendations for the Australian government are:

1. **The Australian Government should implement more rigorous data privacy and data protection legislation**

Too much of the public discussion about the risks of TikTok has been narrowly focused on data security. Even if TikTok were to completely sever access to its user data from China (which it does not plan to do), China's intelligence services could still buy similar user data from data brokers.

It therefore would be to Australia's benefit if more rigorous data privacy and data protection legislation were introduced that apply to all firms operating here regardless of ownership. If protecting national security and guarding against foreign interference are our goals, a broad approach such as this is necessary.

But a complete overhaul of regulation around data will still not address the risk that the CCP could leverage its overwhelming influence over TikTok and its parent company ByteDance in order to manipulate Australia's political discourse in such a way that would unlikely be detected.

There is no technical fix to a problem that is driven by ideology. The CCP considers the country's lack of soft power or "international discourse power" (国际话语权), as having a "discourse deficit" (话语赤字) against the strength of Western media and governments, which in turn has a serious impact on China's international ambitions.[39] The party is open about its view that homegrown social media apps

[37] Juro Osawa and Shai Oster. 'Beijing Tightens Grip on ByteDance by Quietly Taking Stake, China Board Seat', *The Information,* 16 August 2021, online.
[38] Liza Lin and Raffaele Huang. 'TikTok's Talks With U.S. Have an Unofficial Player: China', *Wall Street Journal,* 14 February 2023, online.
[39] Kevin Schoenmakers & Claire Liu. 'China's Telling Twitter Story', *China Media Project,* 18 January 2021, online.

like TikTok present the opportunity to leapfrog the West and begin to meaningfully close that gap.[40] In the past they have attempted to conduct their influence operations on Western social media apps in a process referred to as “Borrowing a boat out to sea" (借船出海).[41] With TikTok, they own the boat.

2. The Australian Government should incorporate countering cyber-enabled foreign interference into cybersecurity and national security strategies.

Countering foreign interference through social media has largely been left to social media platforms and civil society fact-checkers but the Australian Government needs to lead on the issue. Countering cyber-enabled foreign interference should be incorporated into broader cybersecurity and national security strategies. These strategies need to ensure clarity on which government institutions are responsible for dealing with cyber-enabled foreign interference from both an operational and policy perspective. Currently, uncertainty as to whom in government has responsibility is creating a disincentive for victims to report while not providing disincentives to perpetrators to cease their malicious activity. In Australia, the departments of Home Affairs and Foreign Affairs and Trade need to coordinate and lead on implementing policies to build greater deterrence and resilience while the intelligence and law enforcement community need to publicly explain who Australians can turn to for support. Lack of transparency over policy and operational remit is only assisting those with malign intent and harming both Australians and our institutions.

Signals intelligence agencies and cybersecurity centres should play more offensive and proactive roles to deter cyber-enabled foreign interference (as US Cyber Command did in order to signal a willingness to respond to Russian election interference with offensive cyber operations, in this instance temporarily degrading the Internet Research Agency’s infrastructure in 2018[42]). Most countermeasures for combating cyber-enabled influence operations focus on the human element of the information ecosystem, such as fact-checking, capacity building or constructing counter-narratives.[43] Cyber-enabled influence operations, however, should also be considered a cybersecurity issue and more consideration should be given to disrupting the underlying digital infrastructure that enables these operations.

We recognise the challenge posed to policymakers and politicians in Australia given the overwhelming majority of cyber-enabled foreign interference carried out in this region is by China-based or sponsored actors. Any focus on this issue will automatically be viewed as a focus on the CCP. However,

[40] Lin Shujuan (林淑娟) ‘'The Enlightenment of "Two-Level Communication" to International Communication Practice in the New Era"’ (“两级传播”对新时期国际传播 实践的启示)*International Communications (*对外传播*)*, online.
[41] Nathan Beauchamp-Mustafaga & Michael S. Chase. ‘Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations’ *Rand Corporation*, 14 May 2021, online.
[42] Ellen Nakashima, ‘U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms’ *The Washington Post*, 27 February 2019, online.
[43] Laura Courchesne, Julia Ilhardt and Jacob N. Shapiro, ‘Review of social science research on the impact of countermeasures against influence operations’, *Harvard Kennedy School Misinformation Review*, 13 September 2021, online.

a silent approach, even if there is much work going on in classified communities, has proven inadequate to deal with this systemic issue that has impacted individuals, communities and our democratic institutions. As technology continues to advance, so too does the abuse of technology for foreign interference purposes and it is time for Australia's security strategies to increase transparency.

3. The Australian Government should consider mandating platforms to disclose cyber-enabled foreign interference activity.

Unlike traditional foreign interference and espionage, covert foreign interference online can be difficult to attribute and often lack visibility to instigate investigations. In most cases, attribution requires confirmation from the social media platforms themselves which have access to private technical information that is not publicly available. Additionally, the current financial incentive structure of social media platforms means that identifying and removing covert state-backed networks is a lower priority than generating engagement for advertising revenue. While some platforms, including Twitter, Facebook and Google, disclose such activity, others like TikTok and WeChat don't, or do so rarely.

ASPI has previously recommended that an explicit social contract should be developed that holds social media companies operating in Australia to account.[44] This licence to operate should consider mandating social media platforms to disclose state-backed influence operations and other transparency reporting to increase public awareness. While there are differences in the content and impact, data-breach notification requirements around the world could provide a template for how policymakers build a system requiring social media platforms to disclose state-backed inauthentic activity on their platforms. Financial penalties should apply to platforms that fail to disclose malicious activity and platforms should be suspended if there is persistent negligence of the issue. Australian government agencies will have to improve their understanding of state-backed influence operations on social media to audit the compliance of platforms.

This licence to operate could also establish an Australian transparency and oversight board for all social media platforms, which could be involved in setting boundaries and communicating with the public.

4. The Australian Government should provide more specific definitions surrounding ambiguous terms in the DIGI Code

The Australian government changed the definition of "harm" in the DIGI code in December 2022 from "serious and imminent" to "serious and credible".[45] Although this change lowers the threshold for what is considered to be harmful content online, the code leaves the decision to remove harmful content subject to human review, creating ambiguity as to what qualifies. Similarly, while the code

[44] See Danielle Cave and Tom Uren's chapter on 'Influence operations and election interference' in: 'Agenda for change 2019', *ASPI*, February 2019, online.
[45] 'Digital Industry Strengthens Misinformation Code in Response to Community Feedback' *DIGI,* 22 December 2022, online.

very narrowly outlines the definition of harmful as threats to political and policy-making processes, public goods, and protection of citizens' security, it provides no litmus test for what qualifies as "serious".

The DIGI Code has made progressive steps toward combating misinformation by placing clear responsibilities on social media platforms to prevent the monetization of disinformation or the spread of misinformation online. However, the definition of these terms still needs to be more clearly defined for the code to be effective. Similarly, the transparency reports required of social media companies as a result of their participation in the code have proven to be unclear.[46]

Major social media platforms rely on provocative content to increase traffic and revenue to their sites;[47] Therefore, it should not be left up to social media companies to explicitly define these terms just as TV networks are not left to decide what can be aired on national television. The Australian Government should examine similar, offline laws regarding what are considered threats or bullying to further define the terms for social media platforms in the DIGI Code.[48] This would reduce foreign interference through social media by providing more control over reducing the harassment of individuals online and provide continuity amongst human reviewers on what is considered "serious and credible" threats rather than leaving it to personal subjectivity.

5. **The Australian Government should make public diplomacy and deterrence core aspects of countering cyber-enabled foreign interference.**

It is accepted that some action to counter foreign interference must be carried out in secret by our intelligence agencies and government. However, at times the best way to counter disinformation or mitigate threats from cyber-enabled foreign interference is to ensure the public has the necessary facts to make informed judgments. Australian diplomats and intelligence agencies should further collaborate to emphasise intelligence diplomacy with partners in the Indo-Pacific by sharing intelligence on cyber-enabled foreign interference and influence operations. Intelligence based on open-source information, for example, should be more readily shared with partners to build regional resilience and capacity.

The Australian government should coordinate with other partners in the region to name and shame malign actors to increase deterrence. Any public condemnation will, of course, require verifiable evidence to persuade other countries to join and may require declassifying intelligence, in certain circumstances, to support claims.

---

[46] Uri Gal 'Transparency reports' from tech giants are vague on how they're combating misinformation. It's time for legislation' *The Conversation,* 10 Jun 2022, online.

[47] Karen Hao. 'How Facebook and Google fund global misinformation'. *MIT Technology Review,* 20 Nov 2021, online.

[48] 'Cyberbullying and Threats' *Commonwealth Director of Public Prosecution (CDPP),* online.

The Australian government and its agencies, however, should not limit public messaging on this malicious behaviour to cases where there is undeniable evidence of the specific entity that is linked to the activity. Too often, the inability to prove without a question of a doubt who is behind the online activity is resulting in inaction or is used by governments as an excuse to not name individuals or entities within countries or the countries themselves. Even in the offline world, the proof required in both civil and even criminal suits is not beyond any doubt, but rather on the balance of possibilities or beyond a reasonable doubt.

The Australian government should raise its concerns about transnational repression with respective authoritarian regimes or summon their ambassadors. Should such dialogue not change the malicious behaviour against Australian citizens, economic sanctions should be placed on entities involved in foreign interference operations.

6. Law enforcement should work with social media platforms to increase public awareness of transnational repression

The Australian Federal Police (AFP) should implement a public awareness campaign and reporting scheme to counter transnational repression. The AFP could adopt a similar policy as the FBI in the US, which included placing ads on social media asking for individuals to come forward who've experienced harassment on social media from state actors.[49] Law enforcement and intelligence agencies should also step up their community engagement to reassure targeted individuals and marginalised groups. This will help ensure, over time, that victims feel supported and not alone.

Australian government officials and law enforcement need to take activities and communities on social media seriously. Social media has created an unprecedentedly connected global community but this extensive reach has also allowed malign actors to intimidate, coerce and threaten violence beyond their borders, often with impunity and anonymity. Online violence, which is often dismissed as being intangible, must be recognised as having a real impact on the psychological states and mental health of the targeted individuals. Inaction in this area, including by not treating the activity as cyber-enabled foreign interference, only serves to reduce the trust Australians have in our democratic institutions and agencies which both incentivises the perpetrators of harm and helps them to achieve their ultimate goal of Australian disunity.

[49] Lachlan Markay, 'FBI seeks victims of China's overseas pressure campaign', *AXIOS*, 11 January 2023, online.