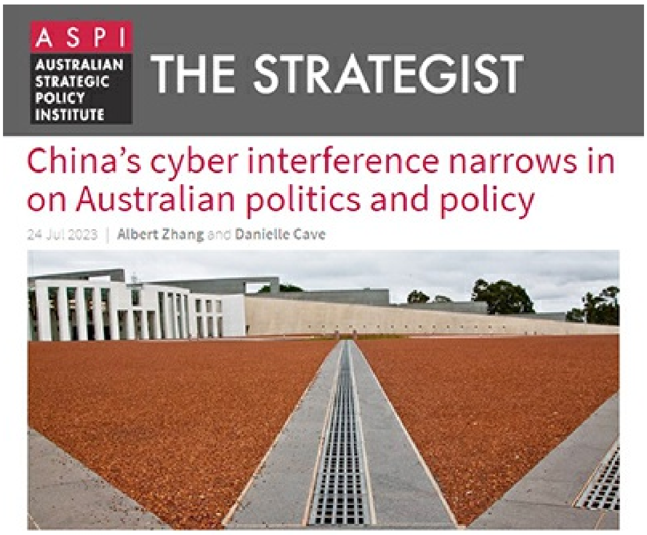
ASPI central in global censorship network

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 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

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.

‘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, 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. 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. 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.

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?

By Melissa Harrison, Australian Alert Service, 9 August 2023