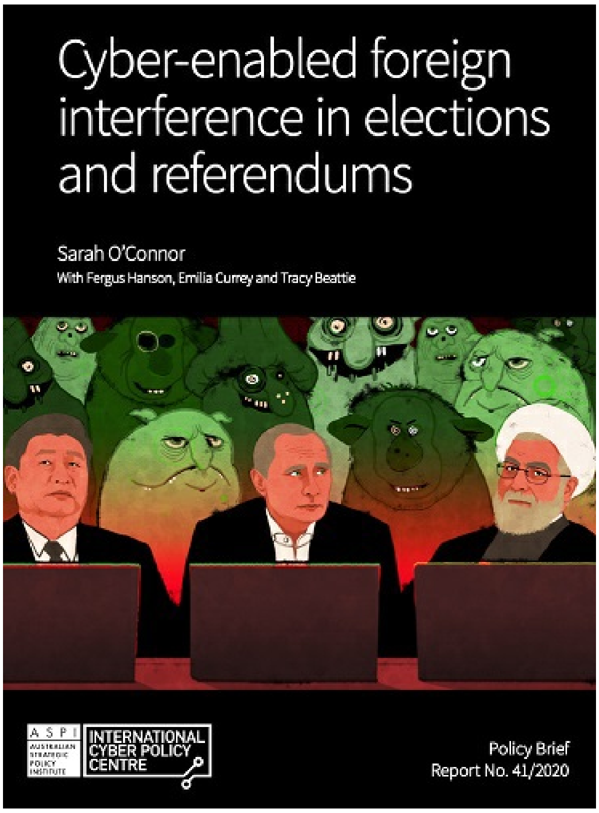
ASPI’s ‘cyber-interference’ allegations: more junk research

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



Cyber-enabled foreign interference in elections and referendums

Sarah O’Connor

With Fergus Hanson, Emilia Currey and Tracy Beattie

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 41/2020

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 Departmentfunded “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 statebacked 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. A

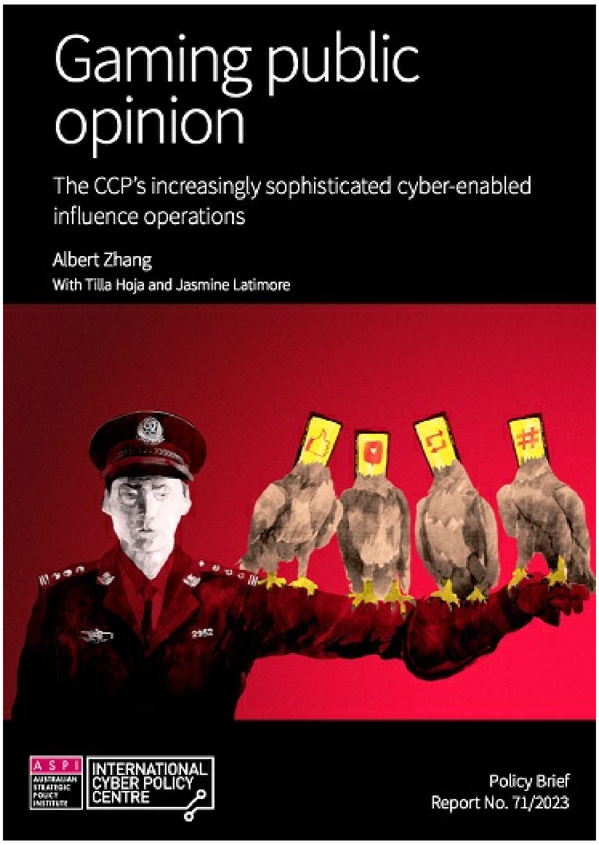
SPI claimed that this supposed Chinese state-backed bot network was linked to “transnational criminal organisations”, suggesting that the Chinese government was now utilising organised crime networks to conduct its cyber-influence operations. However, this sensational allegation was based solely on ASPI’s 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 Opinio*n, 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. 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 socalled 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”.



Gaming public opinion

The CCP’s increasingly sophisticated cyber-enabled influence operations

Albert Zhang
With Tilla Hoja and Jasmine Latimore

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 71/2023

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 AIgenerated 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 MPSaffiliated individuals are directly operating Spamouflage accounts.”

By Melissa Harrison, Australian Alert Service, 16 August 2023