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

About the authors

Albert Zhang is an analyst with ASPI's International Cyber Policy Centre.

Tilla Hoja is a researcher with ASPI's International Cyber Policy Centre.

Jasmine Latimore was a research intern at ASPI in 2022.

Acknowledgements

ASPI acknowledges the Ngunnawal and Ngambri peoples, who are the traditional owners and custodians of the land upon which this work was prepared, and their continuing connection to land, waters and community. We pay our respects to their cultures, country and elders past, present and emerging.

The authors would like to thank all of those who peer-reviewed and provided valuable feedback to improve this report. Thank you especially to Daria Impiombato, Yvonne Lau, Matthew Knight, Jacob Wallis, Danielle Cave, Alexandra Caples and our anonymous external reviewers from industry and government.

Funding for this project came from the US State Department's Global Engagement Center.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies and issues related to information and foreign interference and focuses on the impact those issues have on broader strategic policy. The centre has a growing mixture of expertise and skills, including teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity-building, satellite analysis, surveillance and China-related issues. The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The centre enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and the Indo-Pacific region, the ICPC has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public and private sectors. We thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre, contact: icpc@aspi.org.au.

Important disclaimer

ASPI

Tel Canberra: +61 2 6270 5100
Tel Washington DC: +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published April 2023.

ISSN 2209-9689 (online).
ISSN 2209-9670 (print).

Cover image: Illustration by artist Badiucao, http://www.badiucao.com.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

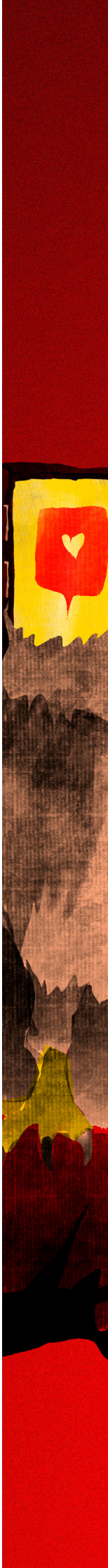
INTERNATIONAL CYBER POLICY CENTRE

Funding for this report was provided by the US State Department.

Gaming public opinion

The CCP's increasingly sophisticated cyber-enabled influence operations

Albert Zhang
With Tilla Hoja and Jasmine Latimore



Policy Brief
Report No. 71/2023

Contents

What's the problem?

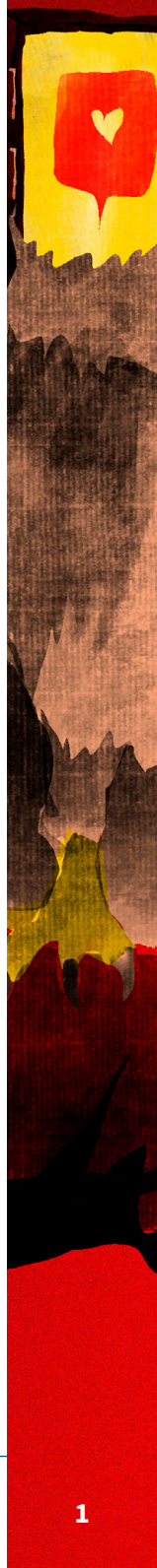
The Chinese Communist Party's (CCP's) embrace of large-scale online influence operations and spreading of disinformation on Western social-media platforms has escalated since the first major attribution from Silicon Valley companies in 2019. While Chinese public diplomacy may have shifted to a softer tone in 2023 after many years of wolf-warrior online rhetoric, the Chinese Government continues to conduct global covert cyber-enabled influence operations. Those operations are now more frequent, increasingly sophisticated and increasingly effective in supporting the CCP's strategic goals. They focus on disrupting the domestic, foreign, security and defence policies of foreign countries, and most of all they target democracies.

Currently—in targeted democracies—most political leaders, policymakers, businesses, civil society groups and publics have little understanding of how the CCP currently engages in clandestine activities online in their countries, even though this activity is escalating and evolving quickly. The stakes are high for democracies, given the indispensability of the internet and their reliance on open online spaces, free from interference. Despite years of monitoring covert CCP cyber-enabled influence operations by social-media platforms, governments, and research institutes such as ASPI, definitive public attribution of the actors driving these activities is rare. Covert online operations, by design, are difficult to detect and attribute to state actors. Social-media platforms and governments struggle to devote adequate resources to identifying, preventing and deterring increasing levels of malicious activity, and sometimes they don't want to name and shame the Chinese Government for political, economic and/or commercial reasons.

But when possible, public attribution can play a larger role in deterring malicious actors. Understanding which Chinese Government entities are conducting such operations, and their underlying doctrine, is essential to constructing adequate counter-interference and deterrence strategies. The value of public attribution also goes beyond deterrence. For example, public attribution helps civil society and businesses, which are often the intended targets of online influence operations, to understand the threat landscape and build resilience against malicious activities. It's also important that general publics are given basic information so that they're informed about the contemporary security challenges a country is facing, and public attribution helps to provide that information.

ASPI research in this report—which included specialised data collection spanning Twitter, Facebook, Reddit, Sina Weibo and ByteDance products—reveals a previously unreported CCP cyber-enabled influence operation linked to the Spamouflage network, which is using inauthentic accounts to spread claims that the US is irresponsibly conducting cyber-espionage operations against China and other countries. As a part of this research, we geolocated some of the operators of that network to Yancheng in Jiangsu Province, and we show it's possible that at least some of the operators behind Spamouflage are part of the Yancheng Public Security Bureau.

The CCP's clandestine efforts to influence international public opinion rely on a very different toolkit today compared to its previous tactics of just a few years ago. CCP cyber-enabled influence operations remain part of a broader strategy to shape global public opinion and enhance China's 'international discourse power'. Those efforts have evolved to nudge public opinion towards positions more favourable to the CCP and to interfere in the political decision-making processes of other countries. A greater focus on covert social-media accounts allows the CCP to pursue its interests while providing a plausibly deniable cover. Emerging technologies and China's indigenous cybersecurity industry are also creating new capabilities for the CCP to continue operating clandestinely on Western social platforms.



Left unaddressed, the CCP's increasing investment in cyber-enabled influence operations threatens to successfully influence the economic decision-making of political elites, destabilise social cohesion during times of crisis, sow distrust of leaders or democratic institutions and processes, fracture alliances and partnerships, and deter journalists, researchers and activists from sharing accurate information about China.

What's the solution?

This report provides the first public empirical review of the CCP's clandestine online networks on social-media platforms. We outline seven key policy recommendations for governments and social-media platforms (further details are on page 39):

1. Social-media platforms should take advantage of the digital infrastructure, which they control, to more effectively deter cyber-enabled influence operations. To disrupt future influence operations, social-media platforms could remove access to those analytics for suspicious accounts breaching platform policies, making it difficult for identified malicious actors to measure the effectiveness of influence operations.

2. Social-media platforms should pursue more innovative information-sharing to combat cyber-enabled influence operations. For example, social-media platforms could share more information about the digital infrastructure involved in influence operations, without revealing personally identifiable information.

3. Governments should change their language in speeches and policy documents to describe social-media platforms as critical infrastructure. This would acknowledge the existing importance of those platforms in democracies and would communicate signals to malicious actors that, like cyber operations on the power grid, efforts to interfere in the information ecosystem will be met with proportionate responses.

4. Governments should review foreign interference legislation and consider mandating that social-media platforms disclose state-backed influence operations and other transparency reporting to increase the public's threat awareness.

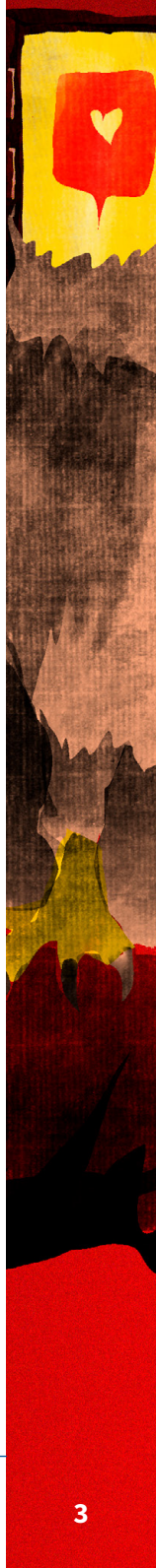
5. Public diplomacy should be a pillar of any counter-malign-influence strategy. Government leaders and diplomats should name and shame attributable malign cyber-enabled influence operations, and those entities involved in their operation (state and non-state) to deter those activities.

6. Partners and allies should strengthen intelligence diplomacy on this emerging security challenge and seek to share more intelligence with one another on such influence operations. Strong open-source intelligence skills and collection capabilities are a crucial part of investigating and attributing these operations, the low classification of which, should making intelligence sharing easier.

7. Governments should support further research on influence operations and other hybrid threats. To build broader situational awareness of hybrid threats across the region, including malign influence operations, democracies should establish an Indo-Pacific hybrid threats centre.

Key findings

- The CCP has developed a sophisticated, persistent capability to sustain coordinated networks of personas on social-media platforms to spread disinformation, wage public-opinion warfare and support its own diplomatic messaging, economic coercion and other levers of state power. That capability is evolving and has expanded to push a wider range of narratives to a growing international audience with the Indo-Pacific a key target. The CCP has used these cyber-enabled influence operations to seek to interfere in US politics, Australian politics and national security decisions, undermine the Quad and Japanese defence policies and impose costs on Australian and North American rare-earth mining companies.
- CCP cyber-enabled influence operations are probably conducted, in parallel if not collectively, by multiple Chinese party-state agencies. Those agencies appear at times to collaborate with private Chinese companies. The most notable actors that are likely to be conducting such operations include the People's Liberation Army's Strategic Support Force (PLASSF), which conducts cyber operations as part of the PLA's political warfare; the Ministry of State Security (MSS), which conducts covert operations for state security; the Central Propaganda Department, which oversees China's domestic and foreign propaganda efforts; the Ministry of Public Security (MPS), which enforces China's internet laws; and the Cyberspace Administration of China (CAC), which regulates China's internet ecosystem. Chinese state media outlets and Ministry of Foreign Affairs (MFA) officials are also running clandestine operations that seek to amplify their own overt propaganda and influence activities.
- Starting in 2021, a previously unreported CCP cyber-enabled influence operation has been disseminating narratives that the CIA and National Security Agency are 'irresponsibly conducting cyber-espionage operations against China and other countries'. ASPI isn't in a position to verify US intelligence agency activities. However, the means used to disseminate the counter-US narrative—this campaign appears to be partly driven by the pro-CCP coordinated inauthentic network known as Spamouflage—strongly suggests an influence operation. ASPI's research suggests that at least some operators behind the campaign are affiliated with the MPS, or are 'internet commentators' hired by the CAC, which may have named this campaign 'Operation Honey Badger'. The evidence indicates that the Chinese Government probably intended to influence Southeast Asian markets and other countries involved in the Belt and Road Initiative to support the expansion of Chinese cybersecurity companies in those regions.
- Chinese cybersecurity company Qi An Xin (奇安信) appears at times it may be supporting the influence operation. The company has the capacity to seed disinformation about advanced persistent threats to its clients in Southeast Asia and other countries. It's deeply connected with Chinese intelligence, military and security services and plays an important role in China's cybersecurity and state security strategies.



Introduction

This report explores the growing challenges posed by China's globally focused and increasingly sophisticated cyber-enabled influence operations, which ASPI defines broadly as planned actions to influence individuals, communities and governments using the cyber domain. Those actions include a range of state-sanctioned activities targeting foreign countries (sometimes individually or as a region) that seek to guide and interfere in their public discourse, to promote disinformation and to threaten and harass individuals and groups. Those activities are typically conducted on social-media platforms, where they're also referred to by industry and national security stakeholders as coordinated inauthentic behaviour,[1] information operations,[2] cognitive domain operations,[3] information warfare or public opinion warfare.[4]

In the first section of this report, which starts immediately below, we review the existing evidence of clandestine cyber-enabled influence operations originating from China to provide an assessment of the CCP's evolving capabilities. By analysing datasets disclosed by social-media platforms and other publicly available sources, we map the CCP's online networks and expose the wide range of Chinese state actors operating covertly on social media and other platforms.

In the second section (from page 11), we present original, empirical research about a recent coordinated CCP propaganda campaign named 'Operation Honey Badger' (蜜獾行动) by Chinese government-linked entities. As of April 2023, this campaign continues to attribute cyber-espionage operations to the US Government. We uncover new evidence to suggest that the MPS, with the support of cybersecurity company Qi An Xin,[5] may be involved in this campaign. This section is highly technical and detailed and sets out an evidence base for subsequent strategic assessments.

In the last section (from page 37), we explain how the CCP's cyber-enabled influence operations are part of a broader strategy to achieve its objectives on social media. This section and our recommendations will be most relevant to policymakers. Our methodology and its limitations can be found in Appendix 1.

China's cyber-enabled influence operations

This report focuses on the CCP's clandestine activities online, as opposed to its overt propaganda system, which has already been extensively mapped and researched. China Media Project, Stanford University and ASPI have all analysed how the CCP, under Xi Jinping (习近平), is pursuing an aggressive external propaganda strategy to 'tell China's story well' (讲好中国故事) and enhance China's 'international discourse power' (国际话语权).[6] This includes the expansion of traditional Chinese media outlets and broadcasters globally[7] and co-opting foreigners and ethnic-minority influencers to speak positively for China,[8] and is part of a broader strategy to transform the liberal international system to favour the CCP's interests.[9]

Understanding the challenge of Beijing's clandestine cyber-enabled influence operations online, however, has been more difficult and largely neglected by democratic governments outside of election periods. The only publicly available datasets covering those activities have been disclosed

by social-media platforms, sporadic leaks of Chinese Government documents and collections of public procurement contracts, which are often deleted after public attention has been drawn to them. The scale and complexity of the datasets sometimes means that only a few research teams globally have the capability and right mix of language, analytical, technical and data skill sets to process them.[10] Nonetheless, the datasets are essential in forming initial assessments of China's evolving cyber-enabled influence capability.

The evolution of Spamouflage

Between August 2017 and December 2022, we identified at least 51 publicly available reports of cyber-enabled influence operations linked to CCP actors published by think tanks, academia and private firms. The full list of the reports is in Appendix 2. We've summarised the reports below to provide an assessment of the trajectory of these operations.

Most US-based social-media companies disclosed Chinese Government-linked covert operations on their platforms, but only Twitter and Meta have previously made the datasets supporting their attributions publicly available (although those disclosures have dried up in 2022–23—the last dataset associated with a network originating from the PRC was disclosed by Twitter in October 2022). In addition, evidence of unreported malign activity on TikTok and WeChat highlights the need for greater government intervention and guidance to apply more consistent policies across all social-media platforms.[11]

Twitter and Meta first attributed inauthentic accounts originating from within the PRC in 2019, but, as ASPI reported in September 2019 research, that network was active as early as 2017.[12] Social-media analytics firm Graphika originally gave the moniker 'Spamouflage Dragon' to this cross-platform network disclosed by Twitter and Meta because the network was composed of fake or hijacked accounts that posted mostly spam before shifting their attention to political topics.[13] Spamouflage Dragon was later shortened to the more commonly-known label 'Spamouflage' (Figure 1). This same network is also known as 'DRAGONBRIDGE', which cybersecurity firm Mandiant claims it had already named earlier in reporting to clients in June 2019.[14]

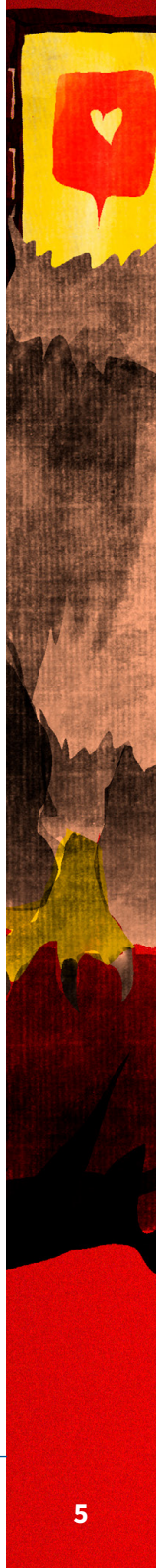


Figure 1: A TikTok account linked to the CCP-linked Spamouflage network

Chinese Transnational Policing Gone Wild **#UyghurHumanRights**

original sound - arzam1015

arzam1015
arzam1015 · 9-22

Follow

Source: TikTok (archived).

The Spamouflage network originally sought to shape narratives about the Hong Kong protests but also supported police-related investigations into dissidents.[15] Twitter found 'reliable evidence to support that [these campaigns were] a coordinated state-backed operation.'[16] Meta found 'links to individuals associated with the Chinese government'.[17] Over the past five years, Twitter has routinely publicly disclosed the most datasets of any social-media platform, sharing nine datasets of campaigns originating in the PRC; the most recent three datasets were released in October 2022. However, it's unclear whether the frequency of disclosures will continue under Elon Musk's management.[18] Likewise, Meta has made at least five public disclosures of coordinated inauthentic campaigns originating from the PRC (the most recent was in September 2022),[19] and Google's Threat Analysis Group has published at least four reports on campaigns originating from the PRC on Google services (the most recent was in January 2023).[20]

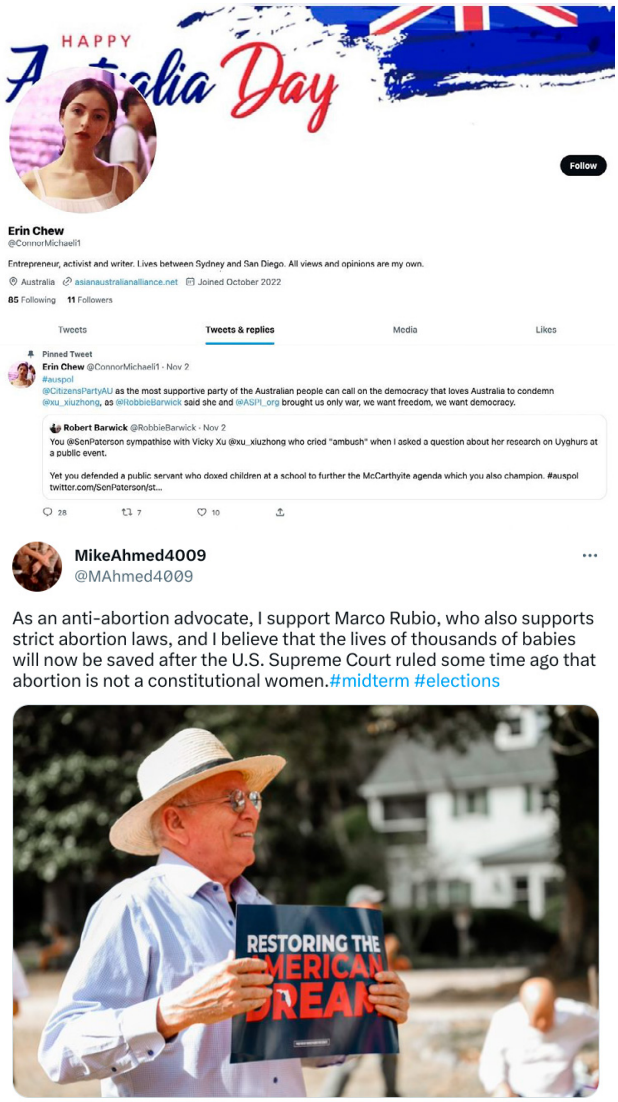
Spamouflage has evolved over the past five years. Not only has it increased in sophistication, but it has expanded to push a wider range of narratives to a growing international audience. When those networks were first discovered, the fake or hijacked accounts had very little engagement with authentic social-media users; almost all engagement was coming from within the network itself. Over the years, major developments in capabilities have driven the network's increasing impact on public opinion.

The Spamouflage network has evolved to focus more on influencing audiences outside China, expanding its early use of predominantly English and Mandarin to content in languages including Russian, Filipino, Korean, French, Japanese, Urdu, Indonesian, Spanish and German. In addition to the

network operating on Western social media platforms, evidence suggests that they operate across at least 40 social media platforms around the world, including Chinese and Russian platforms.[21]

The network has placed increased attention towards developing realistic-looking online personas. For example, accounts within the network posed as members of the operation's target audience's local population, as ASPI and Mandiant observed last year in the Spamouflage-linked rare-earth mining smear campaign, which sought to harm the reputation of Australian and North American mining companies and complicate their efforts to increase rare-earth production.[22] In November 2022, we revealed that Spamouflage accounts were to more directly interfere in Australian politics, seeking to drive online attention to fringe political parties and alt-left political commentators (including some individuals promoting conspiracy theories) in an effort to sow distrust of the government.[23] These accounts engaged in and sparked debates on the state of Australian democracy, Australia–US relations, Australia–China relations and AUKUS. They also made allegations of corruption in Australian politics. Accounts in this network attracted more organic online engagement; their personas appeared more authentic than previous Spamouflage-linked accounts and were sometimes based on real Australian people.[24] For example, one inauthentic account, 'Erin Chew', was based on a real woman named Erin Chew who works at the Asian Australian Alliance advocacy network (Figure 2).[25]

Figure 2: Spamouflage-linked account attempting to interfere in Australian and US politics



Source: Twitter top (archived), bottom (archived).

The network has also expanded the scope of its messaging, moving from predominantly Chinese policing issues to direct, global engagement on a range of political, military and foreign affairs issues. The move to focus on specific issues, coupled with the network's increased reactivity to major geopolitical events, indicates that it's growing more agile. On one occasion, the network even sought to incite people to physical violence in the lead-up to the 2020 Capitol riot in the US.[26] This suggests that the aims of the CCP through these activities are not only to sway public opinion but also to motivate people towards real-world action. As we observed across 2022 and 2023, Spamouflage has successfully shifted to engage in very targeted and misogynistic online harassment campaigns, threatening and intimidating people reporting and working on China, particularly ethnically Asian women living in Western countries and working in high-profile media, human rights and civil society roles.[27] Many of those women have subsequently reduced their online presence or written about the distressing psychological impact of this ongoing experience.[28]

These are concerning developments. So far, researchers have been able to infer Spamouflage-linked campaigns using, for example, key behavioural indicators, links to previous campaigns and accidental leaks of covert operational details. However, that isn't a viable long-term strategy. The CCP appears undeterred in maintaining a presence on Western social media platforms to shape narratives and to enhance its state security, political, economic and military interests. If the Chinese Government makes further improvements to the disguise of its personas, then it may become challenging for analysts to detect their online influence operations. Large language models and other machine-learning applications are also likely to allow the CCP to scale up its clandestine operations and produce more persuasive propaganda narratives.[29]

What we think we know about Chinese covert networks online

Despite years of research and media reporting on Spamouflage, government attribution of the network and other government attribution of covert cyber-enabled influence operations linked to the CCP has been rare (so far, think tanks such as ASPI, social-media platform operators and cybersecurity companies have been relied upon to make such attributions).[30] Understanding which Chinese entities are conducting cyber-enabled influence operations—and their underlying goals and strategies—will be essential in developing approaches to counter their influence. In the following paragraphs, we canvass the publicly available evidence about CCP-linked clandestine networks such as Spamouflage to develop a more nuanced understanding of their activities.

We make some inferences from Spamouflage's behaviour on social media to determine how it operates. Our close examination of Spamouflage accounts finds that they generally have unsophisticated operational security, which suggests that the operation of personas could be contracted out to a commercial firm or internet commentators, rather than directly controlled by security or military officers. For example, accidental leaks of operational details indicate a rushed production process.[31] Further, one Spamouflage account published screenshots of an operator's desktop window instead of properly rendered and exported images.[32] Videos shared by accounts in the network also sometimes appeared to be filmed by mobile devices and unedited, suggesting a low production budget.[33] For similar reasons, RAND Corporation analysts have argued that accounts associated with Spamouflage were not run by the Chinese military but instead likely run by the CCP's Propaganda Department, the United Front Work Department, or both.[34]

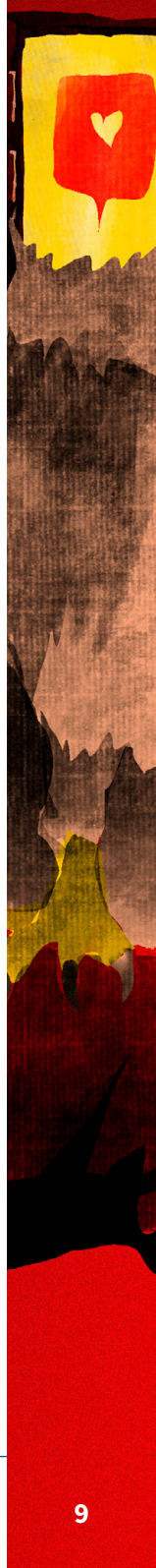
However, the operators of the Spamouflage network are also creating, acquiring, maintaining and purchasing accounts on social-media platforms that invest heavily in cybersecurity and actively defend against platform manipulation. This suggests that there's an investment of talent and resources in Spamouflage activities. After US-based social-media platforms started detecting accounts originating from the PRC, those accounts started using VPN networks to mask their true country of origin.[35] Legitimate social-media users have also had their accounts hacked and repurposed for CCP cyber-enabled influence operations.[36] The scale of the necessary digital infrastructure to sustain these networks requires a sophisticated, technical team that has approval from the Chinese Government to circumvent the Great Firewall.

Public reporting has identified the potential involvement of private Chinese companies in CCP cyber-enabled influence operations in some campaigns. US-based news media outlet *ProPublica* alleged that Spamouflage was linked to a Beijing-based internet marketing company, OneSight Beijing Technology (一网互通北京科技有限公司) in 2020.[37] Its evidence, however, was not conclusive and not corroborated by Twitter.[38]

In addition to the potential involvement of public relations firms, Chinese technology companies are also likely involved in the CCP's covert public-opinion manipulation activities.[39] In late 2021, Meta removed a network of accounts originating from mainland China that had created a fake Swiss biologist, Wilson Edwards, to undermine a renewed World Health Organization investigation into Covid-19's origin in Wuhan, China.[40] Meta found that this network was linked to 'employees of Sichuan Silence Information Technology (四川无声信息技术), an information security firm, and individuals associated with Chinese state infrastructure companies located around the world'.[41] This campaign deserved greater attention than it received at the time, since it demonstrated clear coordination between Chinese diplomats, inauthentic social media accounts, accounts linked to Chinese state-owned enterprises and Chinese state media.[42]

Analysing the CCP's methods to control its domestic information ecosystem offered some insights into its foreign operations. Based on emails leaked from the Zhanggong District Internet Propaganda Office (章贡区网宣办), academics from Harvard University, Stanford University and the University of California, San Diego, estimated in 2017 that there were as many as 2 million internet commentators across the country, popularly known as the '50 Cent Army', that sought to guide public opinion on government-related issues in domestic information spaces.[43] They found that those commentators were mostly lower level government employees posting comments outside their regular job hours to distract the Chinese public, as opposed to outrightly defending the CCP. Local public-security bureaus and the local offices of the CAC have also been reportedly employing their own internet commentators.[44]

Spamouflage campaigns on Western platforms often replicated the tactic of disrupting trending hashtags or flooding online spaces to distract users and 'guide public opinion' (舆论引导). Guiding public opinion is a policy concept that legitimises the CCP's manipulation of domestic information spaces to maintain the stability of the regime.[45] We identified a Spamouflage-affiliated campaign in August 2022 attempting to flood the hashtags #翡翠运动 (#JadeMovement) and #JadeCampaign with content related to Guo Wengui (郭文贵, or Miles Kwok). We assessed that this tactic was intended to drown out calls in the overseas Chinese diaspora, just before the 20th CCP Congress, to overthrow Xi Jinping.[46]



Other CCP cyber-enabled influence operations between 2020 and 2023 were more focused overseas and likely to be political warfare operations conducted by the PLA to interfere with the internal political debates of other countries. Meta disclosed a Chinese information operation in September 2020 that primarily supported President Rodrigo Duterte during the Philippines election and posted content arguing in favour of Chinese regional influence.[47] That network later attacked Taiwan's President Tsai Ing-Wen and posted a small amount of content about the US presidential election. Meta found links between the network and individuals in China's Fujian Province.[48] These campaigns could have potentially been conducted by Base 311 (311基地), which is the PLA's psychological warfare unit in Fujian.[49]

For this research, we also reviewed publicly available Chinese-language academic literature to understand which Chinese agencies were possibly conducting covert campaigns online, but most papers lacked specific details beyond the CCP's broader objective to achieve Chinese discourse power online. A 2021 paper by He Haixiang (何海翔), the Dean of the School of Network Communication at Zhejiang Yuexiu University of Foreign Languages, suggested that an assortment of Chinese Government agencies were possibly responsible for different types of influence operations online.[50] The paper proposes methods for how different Chinese Government entities should compete in a 'US-dominated' international environment. He argues that:

- national and local CAC offices should focus on the guidance of negative international public opinion and establish a team of international online commentators
- national and local propaganda departments should focus on positive guidance, tell China's story well and cultivate influencers and online opinion leaders on overseas social media
- central-level, provincial and municipal state media outlets should 'build ships and go to sea', actively establish new media accounts on social media platforms and export China's soft power
- government cybersecurity departments should actively struggle against Western anti-China forces and hostile organisations, especially at the technical monitoring level, and strive to develop technical monitoring equipment and software to strengthen technical defence.

He Haixiang's views aren't necessarily novel and possibly reflect decision-making that's already occurred within the CCP. His research is informed by consultations with key government departments and security agencies, and the ideas he proposes are probably drawn from such conversations. For example, in 2022, He met with Zhang Yi (张毅), the head of the Cybersecurity Detachment of Shaoxing Public Security Bureau, to discuss integrating the Zhejiang Yuexiu University with the Public Security Bureau to jointly promote the 'safe development of internet public opinion.'[51] In 2019, He met with Xu Weidong (徐卫东), director of the United Front Work Department of the Yuecheng District Party Committee and director of the Yuecheng District Internet Federation.[52]

Another recent paper by scholars at the PLA-affiliated National Defence University[53] argued that Chinese Government agencies focused on domestic governance, private companies and influencers can act as force multipliers for military and intelligence propaganda in times of conflict. The report proposed that, to fight artificial-intelligence-driven 'intelligence public opinion warfare' (智能化舆论战), the Chinese Government should mobilise an integrated linkage of propaganda, public security, foreign affairs, intelligence, military and other departments and cooperate with media, think tanks, international communications and public relations companies and opinion leaders.[54]

The evidence above paints a broad but incomplete picture of the CCP's clandestine online ecosystem. In reality, CCP cyber-enabled influence operations are likely to be conducted by a complicated, integrated ecosystem composed of party-state organisations, state media, military units, and public-security and state-security agencies. In Table 1, we summarise previous public assessments to show the breadth of agencies possibly conducting clandestine influence operations online.

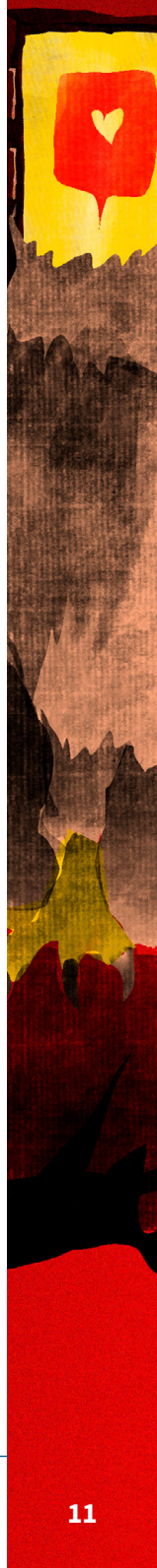
Table 1: The CCP cyber-enabled overseas influence ecosystem

Government entity	Type of covert online activity
Central Propaganda Department	Purchasing and/or creating accounts to amplify online content.[55]
Ministry of Foreign Affairs (MFA)	Purchasing and/or creating accounts to amplify online content.[56]
Ministry of State Security (MSS)	Coordinated trolling and smear campaigns and foreign interference in the political processes of other states.[57]
Ministry of Public Security (MPS)	Purchasing and/or creating personas online, hiring internet commentators and censoring online content.[58]
People's Liberation Army Strategic Support Force (PLASSF)	Foreign interference in the political processes of other states.[59]
Cyberspace Administration of China (CAC)	Hired internet commentators.[60]
United Front Work Department	Purchasing and/or creating accounts to amplify online content.[61]
Chinese state media	Contracting influencers to spread propaganda, contracting public relations companies and purchasing and/or creating accounts to amplify online content.[62]
Chinese state-owned and private enterprises	Purchasing and/or creating personas to amplify content.[63]
Communist Youth League	Coordinating internet commentators.[64]

Case study: Operation Honey Badger (蜜獾行动)

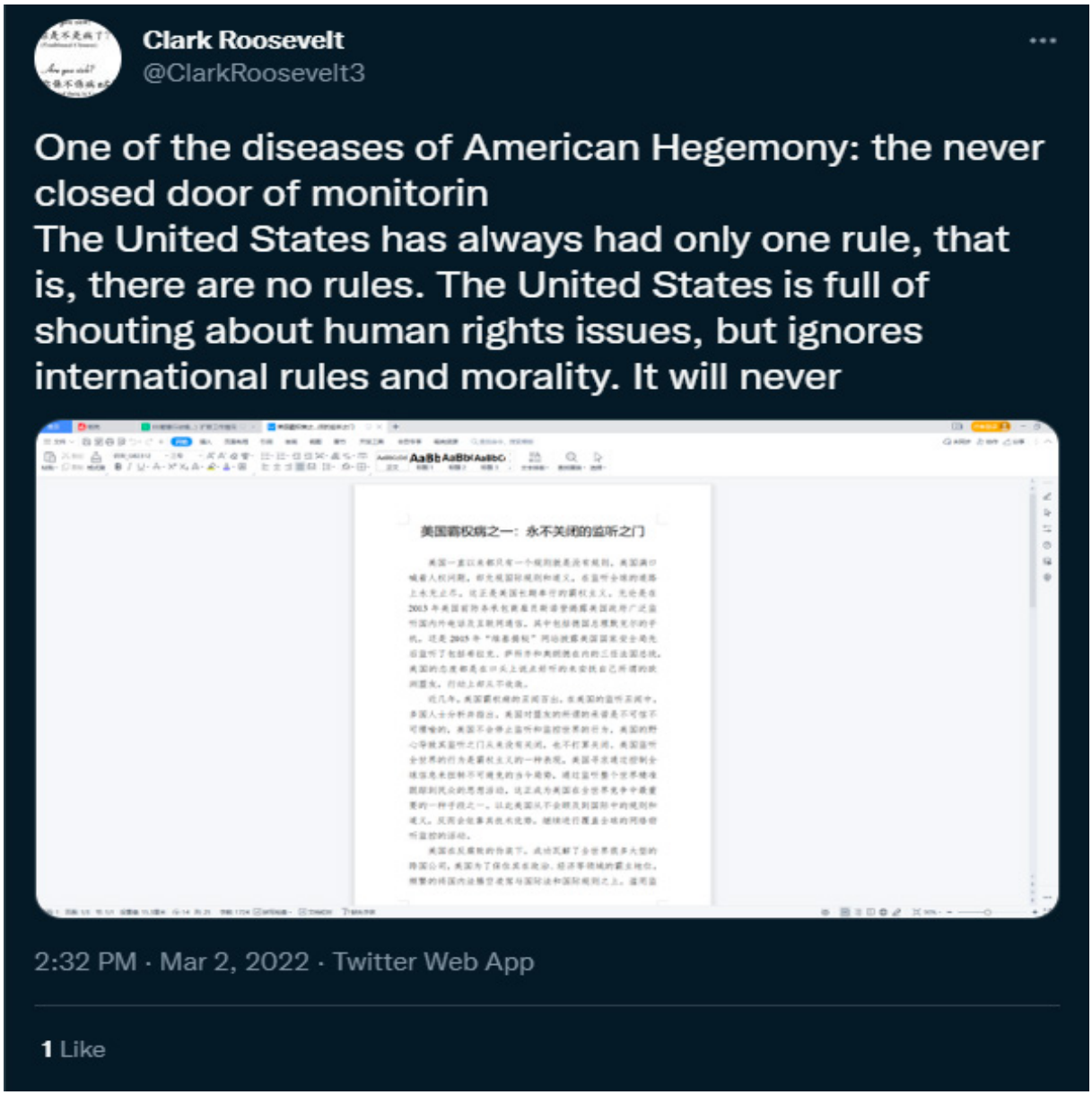
This section investigates a previously unreported CCP cyber-enabled influence operation, linked to the Spamouflage network, that started in 2021 and was ongoing at the time of publication in April 2023. This operation disseminated narratives that the US Central Intelligence Agency (CIA) and National Security Agency (NSA) were irresponsibly conducting cyber-espionage operations against China and other countries. We were unable to verify the claims about US intelligence agencies but believe that those narratives were probably part of a propaganda campaign to support the expansion of Chinese cybersecurity services into Southeast Asian markets and other countries involved in the Belt and Road Initiative (BRI). It also possibly sought to counter similar accusations of Chinese cyber-espionage operations that negatively portray the CCP.

We first analyse public announcements by Chinese Government officials, reporting by Chinese state media and reports published by Chinese cybersecurity companies. We then present original, empirical evidence of inauthentic accounts amplifying those claims across Twitter, Facebook, Reddit, VK, Medium, Sina Weibo and ByteDance products to show that this campaign was coordinated between both overt and covert elements of the CCP's security and propaganda system. Those accounts displayed similar behavioural characteristics to the Spamouflage network, which was previously linked to the Chinese Government by Twitter and Meta, such as by the sharing of identical content used in previously linked Spamouflage campaigns, the use of Western personas,[65] female profile photos,[66] and posting during Beijing time-zone business hours (see Figure 11).



By deep diving into this case study, we build upon the publicly available evidence base of CCP cyber-enabled influence operations discussed in the previous section and shed more light on how those campaigns are conducted. We present evidence suggesting that the MPS, coordinating on its own or acting with prefecture-level offices of the CAC, is likely to have hired internet commentators to post on Chinese- and English-language social-media platforms as part of that campaign. According to an open browser tab identified in an accidentally taken screenshot of an operator's web browser (Figure 3), we believe it's possible that these Chinese Government agencies named this propaganda campaign 'Operation Honey Badger.'[67] We also outline some evidence that seems to suggest that the Chinese cybersecurity company Qi An Xin (which is partly owned by a Chinese state-owned enterprise, China Electronics Corporation) may have been involved. Certain parts of this section are highly technical and detailed but provide the necessary evidence to support the strategic assessments we make in the following section.

Figure 3: Screenshot of a post by a Twitter account likely to be affiliated with the CCP

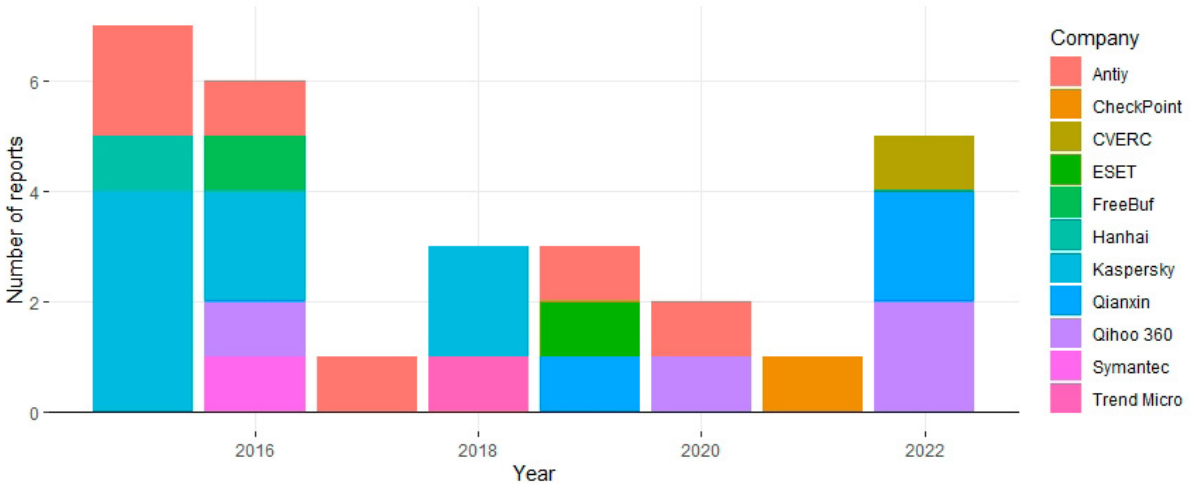


Source: Twitter, archived.

The Chinese Government's public accusations of US cyber-espionage operations relied on key technical reports published by two of China's leading cybersecurity companies: Qi An Xin and Qihoo 360 (奇虎360). On 23 February 2022, Pangu Lab, which is a Chinese security team affiliated with Qi An Xin,[68] claimed that a group linked to the NSA had targeted multiple countries, including China, in a decade-long cyber operation to infiltrate their institutions.[69] In another incident in September 2022, Qihoo 360 and China's National Computer Virus Emergency Response Center (国家计算机病毒应急处理中心) alleged that the NSA had attempted to infiltrate Northwestern Polytechnical University (a Chinese military-affiliated university).[70]

Those claims were part of a growing series of reports attributing malicious cyber-espionage operations to the US Government targeting the PRC and other countries. Between 2015 and 2022, at least 16 reports were published by Chinese cybersecurity companies attributing advanced persistent threats (APTs) to the US (Figure 4). Aside from in 2022, the number of reports per year has decreased since 2015. Reports have been typically issued around a year after major leaks, such as the Edward Snowden leaks between 2013 and 2014[71] (leading to multiple reports being published in 2015), the WikiLeaks publication of Vault 7 (detailing CIA cyber capabilities), and hacker group Shadow Brokers leaks between 2016 and 2017[72] (leading to an increase in US-based APT reports in 2018). The relatively high number of public reports published by Chinese cybersecurity companies in 2022 was then unusual because they didn't directly follow a major US Government leak in the previous year; nor were there corroborating reports from Russian cybersecurity firm Kaspersky, which has occurred in previous incidences of alleged US cyber-operations targeting Russian assets with known tools.

Figure 4: Number of reports per year attributing US cyber operations, by company, 2015 to 2022



Source: ASPI collection and analysis.

Western cybersecurity experts have cast doubts on the veracity of some of those Chinese cybersecurity reports. The attribution of cyber activity to Equation Group, which is an allegedly NSA-affiliated group, in Pangu Lab's report relied on technical indicators that had been public for years and spoofed by other hackers from North Korea, Russia and China. According to *Wired*, Ben Read, director of cyberespionage analysis at US cybersecurity firm Mandiant, says these reports seemed to contain mostly older information from either the Snowden or Shadow Brokers leaks.[73] Netresec, which is a Swedish network security company, also found several errors in Pangu Lab's February 2022 report.[74]

The timing of Chinese cybersecurity reports and the coordinated response from the Chinese Government suggested that the reports were probably part of a propaganda campaign conducted in response to the US Government, NATO, the EU and other allies accusing Beijing of malicious cyber activities in August 2021.[75] Wang Lei, Coordinator for Cyber Affairs of the MFA, said that China believes 'what the US has been doing poses severe damage to China's security interests' and compared those activities to deploying intermediate-range and shorter-range missiles and missile defence systems in China's neighbourhood.[76] In total, we found that China's MFA spokespeople commented on US cyber activities at least 13 times in 2022, and at least 23 articles were published in English online by Chinese state media outlets, such as the *Global Times*, *Xinhua News* and the *People's Daily*, about US cyber operations in 2022.

Coordinated inauthentic behaviour alleging US cyber hegemony

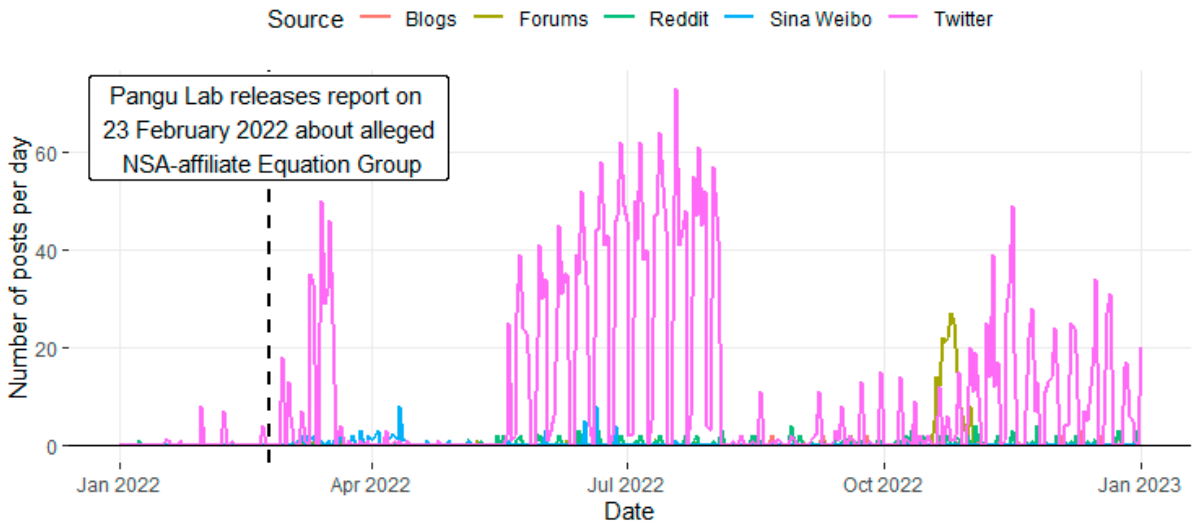
In examining the propaganda campaign, we found inauthentic accounts on Twitter, Facebook, Tumblr, Medium, VK and Reddit disseminating narratives that the US Government was hacking China as far back as mid-2021. For example, a Chinese-language Facebook post published on 4 June 2021 by an inauthentic account probably linked to the Spamouflage network claimed that the US was using its so-called technological advantage to surveil the world (Figure 5; this post attracted 60 shares, likes, and comments).[77] This was one month before the US and allied countries accused the CCP of condoning cyberattacks and suggested that these narratives were already being constructed for another strategic purpose other than countering negative perceptions of China. As of April 2023, some accounts in this network were still active on major social-media platforms such as Twitter, Facebook and Reddit.

Figure 5: Facebook post published on 4 June 2021

Source: Facebook, archived.

For this report, ASPI collected 3,560 tweets, 209 website forum posts, 126 Reddit posts, 37 blog posts, 10 Facebook posts and 71 Sina Weibo posts by accounts believed to be part of the Operation Honey Badger campaign between 1 January 2022 and 1 January 2023. This was a large-scale coordinated cross-platform campaign that persisted for years in multiple languages. Accounts in this network shared the same characteristics as previous Spamouflage-linked accounts, such as the use of Western female personas,[78] sharing the same links and hashtags (such as a fake 'Milk Tea Alliance' report surrounding the origins of Covid-19),[79] posting profile photos generated by artificial intelligence (AI),[80] and posting images criticising Chinese dissident and businessman Guo Wengui.[81] Likewise, the posts were mostly published during the Beijing time-zone work week and business hours. The frequency of posts by accounts in this network peaked directly after Qi An Xin Pangu Lab's report was published on 23 February 2022.

Figure 6: Number of posts per day identified by ASPI between 1 January 2022 and 1 January 2023



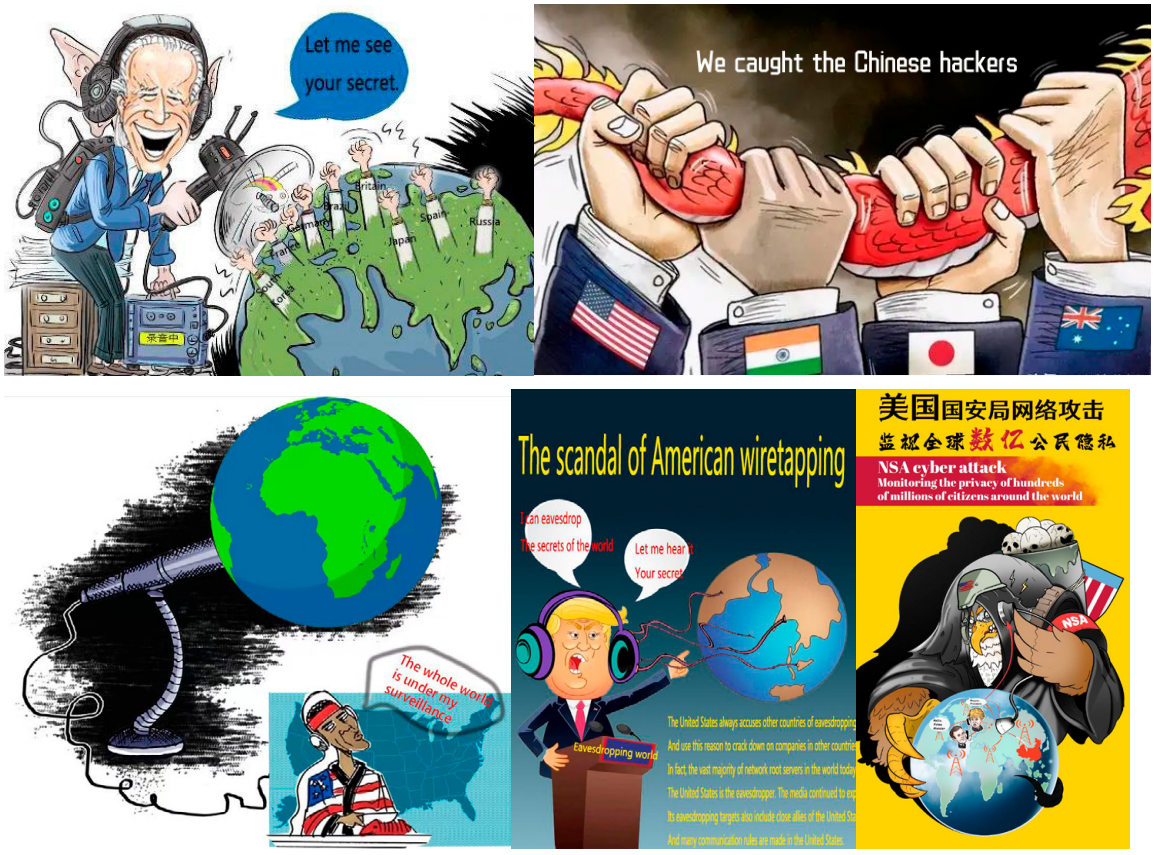
Source: ASPI data collection.

The coordinated covert campaign on social media aimed to amplify the Chinese Government's public announcements and exploited existing distrust of US surveillance operations globally to negatively portray the US Government. For example, many of the posts highlighted details about the PRISM program that were originally leaked by Edward Snowden.[82] The main narratives disseminated by this network included the following:

- The US is a cyber hegemon.
- The US is irresponsibly hacking institutions in China and other countries, including allies.
- The US wants to control global data with the CLOUD Act.[83]
- The US is trying to mislead the international community as a victim of cyberattacks and dominate the international agenda of cybersecurity.
- US Immigration and Customs Enforcement conducts domestic surveillance on Americans.
- Users should take seriously Chinese cybersecurity reports, including Qi An Xin Pangu Lab's report,[84] and products such as Qihoo 360's '360 Security Brain'.[85]

Accounts posted custom images and memes designed specifically to draw attention to US foreign surveillance programs and portrayed China as a victim of false hacking accusations (Figure 7). The artistic style and imagery were similar to those of images shared in previous Spamouflage-linked campaigns, suggesting an element of coordination rather than disparate groups. Some images accidentally revealed that the operators of the accounts were creating images of bulk text by screenshotting their desktop windows rather than properly exporting images. For example, an article titled '美国霸权病之一：永不关闭的监听之门' (One of the diseases of American hegemony: the door of wiretapping that never closes) appears to have been written in WPS Docer, the online version of WPS Office developed by Chinese software company Kingsoft.[86] This article was similar to, but expands upon, a shorter article published by Chinese state media in March 2021.[87]

Figure 7: Examples of images shared by accounts in the network



Source: Collected by ASPI from Twitter.

On Twitter, accounts typically amplified hashtags related to US cyber activity and included a mix of both English- and Chinese-language hashtags. English hashtag examples included #USCyberHegemony, #USsurveillance, #Americancyberhegemony, #EspionageEmpire or #USthreatenscybersecurity. Hashtags in Chinese included #美国黑客入侵别国 (#American hackers invade other countries), #美式霸权 (#American hegemony), #抵制云法案 (#Resist CLOUD Act), #骇客美国 (#Hack America), #霸权主义 (#Hegemony), #黑客帝国 (#The Matrix) and #窃听风云 (#Eavesdropping cloud).

There was strong evidence linking these accounts to another iteration of the Spamouflage network, such as the timeline history of some accounts, which showed that they had previously participated in Spamouflage campaigns that harassed and abused reporters of Asian descent[88] and used the

#GenocideGames hashtag to target Chinese virologist Yan Li Meng (闫丽梦) and exiled Chinese businessman Guo Wengui.[89] Accounts accusing the US of cyber-espionage were also found in an information operation takedown disclosed by Twitter in October 2022 against interference originating from mainland China.[90] That network mostly targeted US civic issues leading up to the US mid-term elections but also amplified Chinese diplomats condemning US cyber operations, promoted Qihoo 360's report on US cyber operations and posted tweets claiming that the US is addicted to 'voyeurism and eavesdropping' to maintain its hegemony.[91]

The distribution of these narratives wasn't limited to inauthentic accounts online but was coordinated with public CCP-affiliated propagandists. In total, Chinese diplomats and government accounts tweeted or retweeted about US cyber operations at least 103 times in 2022. This was problematic because official social-media accounts of Chinese state media and government officials often directly amplified content posted by inauthentic accounts. In one case, the official Twitter account of T-House, which is the opinion section of Chinese state media *CGTN*, posted a tweet that was generated by an account with an AI-generated profile image, which we assessed belonged to the Spamouflage network (Figure 8). This tweet was also repeated by Li Bijian (李碧建), the Consul-General of China to Karachi.[92] These tweets used a Graphika and Stanford Internet Observatory report on a US military-linked social-media influence operation to portray the US Government as a threat to global cybersecurity.[93] Whether it's the US military or the CCP, the use of coordinated inauthentic accounts to artificially spread preferred narratives undermines the ability of all social-media users to form independent opinions.

Figure 8: In chronological order, the official T-House Twitter account posts at 3:38 pm (GMT+8); Lori Gutierrez, a likely Spamouflage account with an AI-generated profile image, then posts at 4:32 pm, (GMT+8) followed by the Consul-General of China to Karachi at 11:12 pm (GMT+8)

Sources: Left, middle, right.

The necessary resources and coordination between Chinese state media, the MFA Information Department, government officials and covert assets online to conduct a large-scale propaganda campaign indicated that these narratives were likely to have been directed, or at least approved, by senior decision-makers within the CCP. Previous comparable propaganda campaigns included efforts to counter criticisms of the CCP's policies in Xinjiang,[94] shape international depictions of the Hong Kong protests,[95] spread disinformation about the origin of Covid-19 and promote the CCP's response to the Covid-19 pandemic.[96] Those issues directly affected the political legitimacy of the CCP and its state security. As with those other propaganda campaigns, the narratives identified in this report

appear to primarily target foreign audiences. Domestic Chinese audiences could have been one target of this messaging, too. Propaganda highlighting the threat of US cyber operations can help justify to Chinese citizens the series of new laws and regulations related to cybersecurity enacted during the Xi regime.[97]

This cross-platform campaign demonstrates two significant advances in the CCP's foreign propaganda capabilities.

First, it shows an appreciation of the messages that Southeast Asian countries, classified as 'understanding and willing partners' in the CCP's precise communication strategy, are likely to be most susceptible to.[98] According to Hu Zhengrong, former Communication University of China dean and the head of the Chinese Academy of Social Sciences' Journalism and Communication Research Institute, China should focus on 'soft' communication and prevent concerns over the 'China threat theory' caused by economic development for willing partners in Southeast Asia.[99] In recent years, Southeast Asian countries have been targeted by Chinese state-sponsored cyber operations, and that activity is undermining efforts by Chinese cybersecurity companies to secure the trust and support of policymakers and markets in the region.[100] To counter concerns about the 'China threat theory' that have slowed Huawei's global expansion, this propaganda campaign emphasises a 'US threat theory' to distract international audiences. It also demonstrates the apparent capabilities of Chinese cybersecurity companies to detect APTs, including US-based ones, which US cybersecurity companies are hesitant to disclose. At a minimum, the 'US cyber threat' narrative argues that there's a moral equivalence between Chinese and US cyber operations. The logic follows that, if the US conducts cyber operations to protect US interests, then China should be able to conduct cyber operations to protect CCP interests. This equivalence allows the CCP to undermine the moral high ground of the US when it accuses the CCP of cyber operations and asserts that the CCP is simply another responsible power exerting its influence in Asia.

Second, posts by inauthentic accounts, public government announcements and state media reporting have based their claims on highly technical, but potentially misleading, reports by Chinese cybersecurity companies. Those reports provided the necessary 'evidence' that narratives could be anchored on. Highly technical reports are also difficult to verify and have the advantage of appearing legitimate initially because most analysts lack the required skills to make definitive assessments. Chinese cybersecurity companies can also appear as independent third-party actors to support broader propaganda narratives. We discuss later in this report how Chinese cybersecurity companies are closely intertwined in Chinese foreign influence operations, which might cast suspicions on the intent of their reports (see 'Connections with Qi An Xin' section below).

Spamouflage accounts on Chinese social-media platforms

This report uncovers for the first time Spamouflage-linked activity on multiple Chinese-language social-media platforms and online forums such as Sina Weibo, Baidu Tieba, Zhihu, Toutiao, Billibilli and other Chinese websites. We first show the connection between activity on Chinese-language platforms and Spamouflage accounts on Western platforms. We then present account location information, the use of personal accounts and the exclusive following of MPS accounts to infer a relationship with the MPS or CAC.

Evidence to suggest that these Chinese social-media accounts were connected to Spamouflage included the fact that those accounts posted exact replicates of screenshots being shared on US-based social media. A screenshot of an article titled '美国霸权病之一：永不关闭的监听之门' ('One of the diseases of American hegemony: the door of wiretapping that never closes') was the most obvious link between different platforms (Figure 9). The screenshots received little engagement on US-based social media and thus were unlikely to be shared by Chinese netizens from Western platforms. By searching for the same screenshots and phrases on Chinese websites, we identified more 200 additional accounts that we could confidently link to Spamouflage. Those accounts 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.

Figure 9: Weibo links to Spamouflage based on replicated images and phrases

Source: (left) Twitter, (right) Sina Weibo.

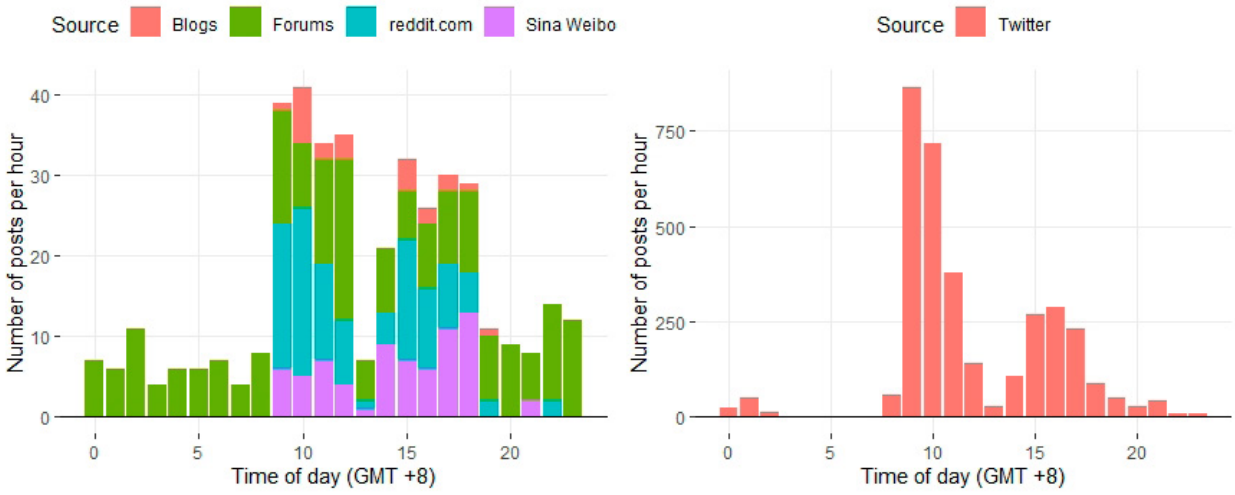
In addition, Chinese social media accounts in this network posted articles attacking and smearing female journalists, researchers and activists of Asian descent based in Western countries. The accounts that mostly posted about US cyber activities also targeted Gu Bo, a *Voice of America* journalist based in the US, and called them a traitor (Figure 10). These campaigns have previously been linked to the Chinese Government.[101]

Figure 10: Spamouflage activity on ByteDance-owned social media platform, Toutiao, and Tumblr explorer, Tumpik

Source: (top) Toutiao, online, archived; (bottom) Tumpik, online.

The posting patterns of the Chinese social-media accounts in this network were closely correlated with Spamouflage-linked accounts on Western social-media platforms. As in previous iterations of the Spamouflage network, almost all Sina Weibo posts were published between Beijing time '996'; that is, during business hours with a break for lunch between 12 pm and 2 pm (GMT +8) (Figure 11).[102] Accounts on Chinese social-media platforms weren't suspended despite displaying clear indications of being inauthentic, suggesting that those platforms didn't prevent Spamouflage activity on Chinese social media and their possible tacit approval by the Chinese Government.

Figure 11: Posting patterns of Spamouflage activity on Twitter, Sina Weibo and other websites. Blogs and forums included both English and Chinese language posts



Note: Blogs and forums included both English and Chinese language posts.
Source: ASPI analysis of collected data.

From the beginning of 2022, major Chinese social-media platforms started displaying user locations based on IP addresses. This compulsory feature was implemented to 'prevent netizens from pretending to be Chinese locals'[103] and potentially unearth foreign disinformation campaigns.[104] The irony of this policy is that it may have helped expose CCP cyber-enabled influence operations on Western social media platforms, too.

Of the posts we identified sharing screenshots of the article titled '美国霸权病之一：永不关闭的监听之门' ('One of the diseases of American hegemony: the door of wiretapping that never closes') and other Spamouflage-related content, technical indicators showed that those accounts were being posted from Jiangsu Province, Hong Kong, Beijing and other regions around China. This matched some of the locations identified by Twitter in a Chinese information operation originating from mainland China in October 2022. A Twitter account involved in a campaign targeting Lynas Rare Earths,[105] and posting about US cyber operations, has also shared an image revealing that its IP location is geolocated to Hong Kong. This was based on the trending topics at the bottom right-hand side of the image window.[106] Using other geolocation tools,[107] we identified an additional eight posts from Yancheng city, Jiangsu, eight from Nanjing, the capital city of Jiangsu, seven from Zhenjiang city, Jiangsu, and five from Beijing. One account named '小橙子的理想' ('The ideal of a small orange' (Figure 12) posted about the CIA's cyber operations and accidentally used Weibo's check-in function to reveal that it was based in Yancheng (Figure 13). This account had a profile image of Taylor Swift and posted only about US cyber operations and other Chinese police-related topics that were shared by other Spamouflage-linked accounts.

Figure 12: Weibo post by user '小橙子的理想' ('The ideal of a small orange') with Yancheng city check-in tag

Source: Weibo, online, archived.

Posts on other Chinese social-media platforms corroborated our hypothesis that some Spamouflage operators were based in Yancheng city. On Zhihu (知乎), which is the Chinese equivalent of Quora, one account named '新垣结衣' (Yui Aragaki) had repetitively posted an article titled '美国霸权病之一' (One of the diseases of American hegemony), and other articles attacking Gu Bo, since at least September 2022.[108] This account appeared to have used its own personal account to disseminate Spamouflage-related content and had not deleted its previous history of activity. Prior to January 2022, Yui Aragaki 'liked' other Zhihu answers about the salary of primary school teachers in Funing County and Xiangshui County in Yancheng and bookmarked articles about registering for self-study examinations in Jiangsu. Under a Zhihu post about a wedding in Yancheng posted by another account, Yui Aragaki answered 'Hey, no matter what, it's still my hometown.'[109]

Some evidence suggests that these accounts were possibly affiliated with the Yancheng Public Security Bureau and the central MPS. One account named '吉娃娃呀吉娃娃' ('Chihuahua Yeah Chihuahua') on Toutiao, a ByteDance-owned social-media platform, had posted only six articles, each about US surveillance, that have been posted only by other Spamouflage accounts on Chinese and English social-media platforms. As of the publication of this report, each article has been read seven times at most, and the account only has four fans, but most of those posts are usually intended to flood the internet rather than get organic engagement. The only other account 'Chihuahua Yeah Chihuahua follows' is the official Toutiao account of the Traffic Police Detachment of Yancheng Public Security Bureau (Figure 13), and its IP location is listed in Jiangsu.[110] For context: the guidance of online public opinion about traffic management has become an aspect of police public-security work after Chinese netizens started uploading videos criticising traffic police on duty.[111]

Figure 13: Screenshot of '吉娃娃呀吉娃娃' Toutiao account

Source: Toutiao, online.

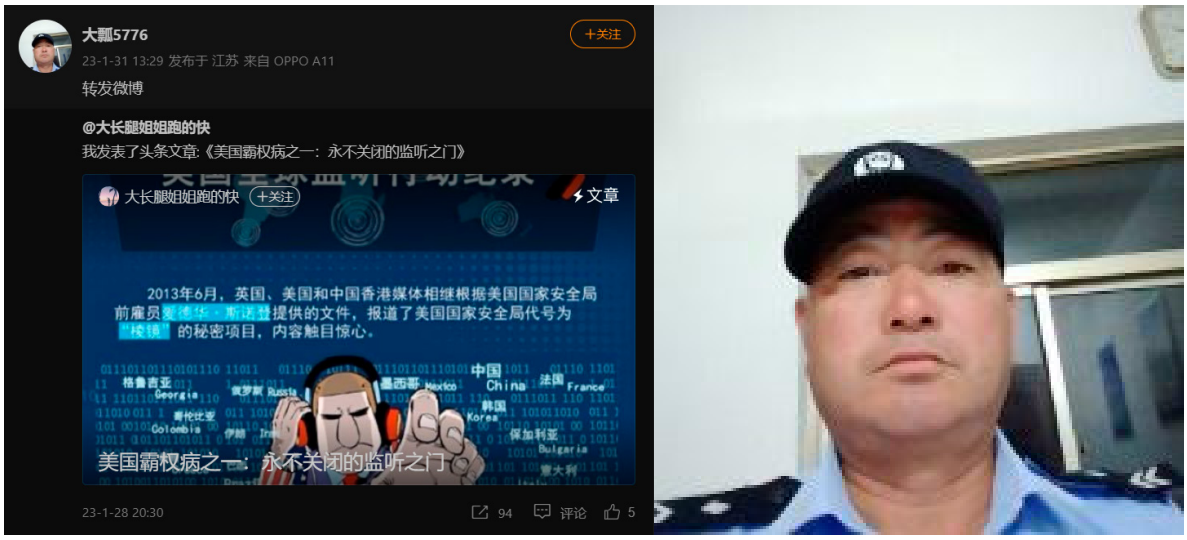
Another Toutiao account named '爸爸68910361' ('Daddy68910361') published 19 articles, each about US surveillance operations or attacking Gu Bo (Figure 14). This account has zero followers, and its IP location is also listed in Jiangsu. The only two accounts 'Daddy68910361' follows are the official Toutiao account of the MPS and 'New Police Matters' (新警事儿) of the *People's Public Security Newspaper*, which is the official propaganda newspaper of the MPS.

Figure 14: Screenshot of '爸爸68910361' Toutiao account

Source: Toutiao, online.

The Washington Post discovered other possible links to Chinese police officers after ASPI shared a list of Weibo accounts that were likely part of the Spamouflage network on Chinese social media.[112] In one case, the Washington Post found another Weibo account which appeared to have a self-taken photo of a Chinese police officer as its profile image (Figure 15). This account was likely part of the Spamouflage network because it's listed IP address suggested it was operating from Jiangsu and the only posts on its timeline were forwarded posts from other Spamouflage-linked accounts about US cyber hegemony.

Figure 15: Screenshot of 'Big Ladle 5776' (大瓢5776) Weibo account and profile image



Source: Weibo, archived.

The Washington Post also identified another Weibo account named 'User7763546981' (用户7763546981), which appeared to have a police station as its profile image and was only forwarding posts from other Spamouflage-linked accounts about US cyber hegemony. The Washington Post geolocated this image to the Gangbei Police Station of the Jianhu County Public Security Bureau in Yancheng, Jiangsu (Figure 16).

Figure 16: Links between 'User7763546981' (用户7763546981) Weibo account and Gangbei Police Station Jianhu County Public Security Bureau in Yancheng, Jiangsu

Source: (top) Weibo, archived, (bottom) Sohu, archived.

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. The CCP's security apparatus is secretive, and we didn't expect to find comprehensive details about its specific operations in open-source channels.

However, as both Twitter and Meta have previously already attributed Spamouflage to the Chinese Government, the addition of the evidence above strongly indicates that China's public-security bureaus are probably some of the key actors within the Chinese propaganda system that's behind the Spamouflage campaigns taking place across US-based and Chinese-based social-media platforms. This could also explain why so many of the earlier Spamouflage campaigns were police-related. The most significant and sustained Spamouflage campaigns on Western social media started targeting Guo Wengui five days after an Interpol red notice was issued at the request of the Chinese Government.[113] ASPI analysts previously found inauthentic accounts directly quoting the Beijing Public Security Bureau in Twitter's August 2019 disclosure of a Chinese state-backed information operation.[114] Spamouflage-linked accounts currently active on Twitter have also posted tweets to counter alleged 'rumours' about police in Xuzhou city in Jiangsu Province.[115]

Yancheng Public Security Bureau is well known for police-related propaganda work. In June 2018, Yancheng city hosted a national public-security propaganda seminar that was attended by some of the MPS's top propaganda and political work brass.[116] Yancheng Public Security Bureau organised training seminars and activities on the CCP's 'public opinion work', strengthening positive government propaganda and improving public security news and propaganda work.[117]

Since 2019, political and legal agencies such as police departments across China have followed Xi Jinping's instructions to comprehensively improve their capacity to guide public opinion and disseminate propaganda.[118] China's political and legal system, which oversees the MPS, is also known for managing 'internet commentators' that manipulate online discourse to protect the political security of the CCP. In 2018, Chen Yixin (陈一新) the Secretary-General of the Central Political and Legal Affairs Commission, openly encouraged political and legal cadres, police officers and propagandists to open social-media accounts to influence online conversations and control which topics trend online.[119]

While police officers were likely involved in coordinating Spamouflage propaganda campaigns, creating content and operating some social-media accounts, it's highly unlikely that they were directly controlling all the inauthentic accounts themselves, since most of the posts were largely published during business hours. When Chinese Government officials, including police officers, have previously commented covertly on Chinese online forums, they would typically post outside their usual work hours.[120] The operation of most personas on social media is possibly outsourced to a specially trained—and ideologically sound—group of 'internet commentators' (or spin doctors)[121] employed by the Yancheng office of the CAC or, alternatively, a commercial firm.[122] News articles confirm that Yancheng CAC uses internet commentators. A 2020 article reported that grassroots cyberspace administration staff and internet commentators were invited to an evaluation conducted by the Yancheng Cyberspace Administration of the city's internet service units.[123] Earlier that year, Dong Guangwei (董光威), Director of the Yancheng CAC and Deputy Director of the Yancheng Propaganda Department insisted that the local government forge a 'cyber iron army' (网信铁军).[124] The Yancheng CAC is also recognised for its public-opinion guidance work. In 2019, it was awarded an Excellence Award for Internet Public Opinion Guidance at the Fifth National Internet Public Opinion Summit

Forum held in Lanzhou City, Gansu.[125] According to the *People's Daily Online*, Yancheng Cyberspace Administration proudly 'guides public opinion, responds rationally to public concerns, and is actively involved in preventing the spread of rumours'.[126]

Profiling the online history of Yui Aragaki's Zhihu account (a Spamouflage-linked account that was based in Yancheng city) supports the hypothesis that the individuals posting Chinese propaganda were probably internet commentators contracted by the local government. The Yui Aragaki account is most likely operated by a young male.[127] He's probably is likely a part-time student living in Yancheng,[128] and unlikely to be a public servant because it's generally difficult for students without a university degree to get those jobs. In an image accidentally shared by another Spamouflage-linked account (an open tab in the operator's browser windows) shows a WPS Office spreadsheet titled 'XX Operation Honey Badger … diffusion work report'.[129] The 'XX' symbol is often used in government document templates as a placeholder for a city in nationwide grassroots work reports.[130] This could possibly explain why some posts on social media were decentralised and distributed to units in different cities.

Police officers, however, closely collaborate with CAC staff to censor content online and supervise internet commentators (Figure 17). By law, there must be at least two law-enforcement officers present when CAC staff conduct content-management investigations and collect evidence online.[131] While the CAC creates policies for regulating cyberspace, the public-security system is responsible for enforcing those policies. For example, the Cybersecurity Department of the MPS has publicly asked on six occasions to censor repositories affiliated with Falun Gong in 2019.[132]

Figure 17: Yancheng Public Security Bureau and the Yancheng Cybersecurity Administration co-hosting a public-opinion security briefing to clean up cyberspace

Source: Sina, archived.

Alternatively, the posting of internet comments could possibly be outsourced to a commercial entity. Yancheng Public Security Bureau has a contract with Smart Starlight Information Technology (北京智慧星光信息技术有限公司), for example, for an online public-opinion monitoring push-notification service.[133] Smart Starlight is based in Beijing and provides monitoring software to Chinese police. [134]

Connections with Qi An Xin

The possible involvement of Chinese public-security bureaus and the CAC in cyber-enabled influence operations would only represent one piece of a larger puzzle. Many of the Spamouflage campaigns active on US social-media platforms and identified since 2017 aren't related to police propaganda work or are about managing domestic online public opinion; they're largely global in nature. For example, PRC-origin influence operations across multiple platforms sought to target the Czech Republic's foreign policy towards China and Ukraine in September 2022.[135]

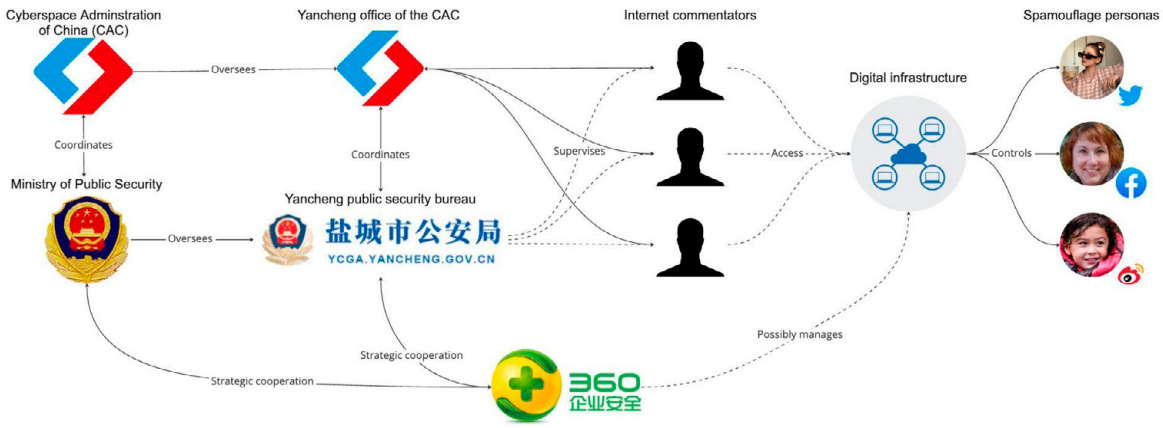
In addition, hacking social media accounts and maintaining a global VPN infrastructure that avoids platform detection requires sophisticated offensive cyber capabilities. In April 2022, the Institute for Strategic Dialogue found that the verified account of the French MP Bernard Reynès and the account of Liliana Pérez Pazo, a local politician in Spain, had been hijacked to spread pro-CCP talking points and were probably affiliated with the Spamouflage network.[136] There's also a growing body of evidence suggesting a possible link between Chinese APT actors and Spamouflage (see Appendix 3 on page 52 for further details).

Below, we present evidence showing that the nexus between offensive cyber capabilities, different types of Spamouflage campaigns and public security propaganda conducted out of Yancheng all point back to Qi An Xin, the cybersecurity company that first allegedly reported about US cyber-espionage operations in February 2022. At the launch of the 'Military–Civil Integrated Innovation Center for Cyberspace Security', Qi An Xin's chairman and party secretary, Qi Xiangdong (齐向东), said that 'chaos evolving out of online public opinion have become global public hazards' and that cybersecurity has a 'bearing on national security, regime solidity, social stability, and the outcome of a war'.[137] Qi Xiangdong is also a member of the Big Data Operation and Maintenance (Cybersecurity) Committee of the All-China Federation of Industry and Commerce, which is an organisation under the leadership of the United Front Work Department.[138] Fan Youshan (樊友山), deputy secretary and vice chairman of the party group of the All-China Federation of Industry and Commerce, suggested that this committee does a good job in controlling public opinion for the CCP and helping China become a 'cyber powerhouse' (网络强国).[139] These statements strongly suggest that Qi An Xin, under Qi Xiangdong's leadership, has the intent to manipulate online public opinion to pursue CCP objectives.

Qi An Xin's links with CCP cyber-enabled influence operations

We begin this section by revealing the links between Qi An Xin, Yancheng Public Security Bureau and other Chinese Government agencies (Figure 18). Those links suggest that Qi An Xin could possibly be providing digital infrastructure support to Chinese Government agencies that conduct clandestine online operations. We present evidence that suggests that Qi An Xin, or one of its subsidiaries, may be affiliated with the Spamouflage network and other clandestine influence operations on Western social-media platforms. Finally we find that Qi An Xin, as part of Operation Honey Badger, is collaborating with former PLA military intelligence assets and is possibly seeding disinformation about APTs to its clients in Southeast Asia and other countries (further details are on page 34).

Figure 18: Summary of the proposed relationship between Spamouflage inauthentic accounts, Chinese Government agencies and Qi An Xin / 360 Enterprise Security Group (360企业安全集团)



Source: ASPI analysis.

Qi An Xin is deeply connected with Chinese intelligence, military and security services and plays an important role in China's cybersecurity and state-security strategies. Qi An Xin was publicly listed in 2019 and is now partly owned by a Chinese state-owned enterprise, China Electronics Corporation (CEC, 中国电子信息产业集团有限公司). CEC was listed by the Trump administration in 2020 as a 'Communist Chinese military company' operating directly or indirectly in the US.[140] See Appendix 4 for further details about Qi An Xin's links to Chinese intelligence, military and security services.

Qi An Xin cooperates with the Yancheng Public Security Bureau, which we've identified as possibly conducting some Spamouflage campaigns on Chinese social media. Qi An Xin was formerly known as 360 Enterprise Security Group (360企业安全集团), a subsidiary within the 360 Group (360集团), before the company split in 2019.[141] While Qi An Xin was still named 360 Enterprise Security Group, it signed a strategic cooperation agreement with Yancheng Public Security Bureau to improve police capabilities and jointly combat internet crime (Figure 19).[142] He Xinfei (何新飞), then vice president of 360 Enterprise Security Group and now vice president of Qi An Xin, said the company will provide cybersecurity services, technical services and police personnel training as part of the agreement.[143] Qi An Xin kept all the government contracts after it split from the 360 Group and probably retained this cooperation agreement with Yancheng Public Security Bureau.[144] In 2020, Qi An Xin provided firewall systems for the governments in Jiangsu Province, including in Yancheng.[145]

Figure 19: He Xinfei, then vice president of 360 Enterprise Security Group, on the left and Wang Qiaoquan, deputy mayor of Yancheng City and director of Yancheng Public Security Bureau, on the right

Source: Sina, archived.

Qi An Xin and Yancheng Public Security also jointly unveiled two new collaboration centres at the signing of the cooperation agreement: the National Laboratory for Big Data Collaborative Security Technology to Prevent and Combat Cybercrimes Collaboration Centre (大数据协同安全技术国家实验室涉网犯罪预防与打击合作中心) and the Cybercrime Prevention and Combat (Belt and Road) International Cooperation Research Centre (网络违法犯罪预防与打击(一带一路)国际合作研究中心).[146] Those laboratories are part of a series of national laboratories that bring together public-security officers, military personnel and other experts to collaborate on big-data technology applications such as public-opinion monitoring.[147] At a closed-door seminar at the National Engineering Laboratory of Big Data Collaborative Security Technology in Beijing, Major General Hu Xiaofeng (胡晓峰), former deputy director of the Department of Information Operations and Command Training at the National Defense University, said he was optimistic that the laboratory could 'represent the country, have a Chinese voice and strive to be unique in the international arena'.[148]

Qi An Xin chairman Qi Xiangdong (齐向东), was appointed the Director of the National Engineering Laboratory for Big Data Collaborative Security Technology at its founding in 2017.[149] That probably positioned the cybersecurity company conveniently to provide underlying digital infrastructure to support Chinese military, intelligence and security agencies.[150] According to Qi An Xin's 2021 annual report, over 40% of its main revenue comes from government and law-enforcement agencies, and its clients also include users from the military and the defence industry.[151]

Typically, 'public-opinion guidance work' is carried out by Chinese state media, but it's also a public-security issue that involves companies such as Qi An Xin.[152] Qi An Xin representatives have previously presented at Chinese Government seminars that consider online public-opinion guidance

as a form of cybersecurity. For example, at an August 2020 Inner Mongolia Association for Science and Technology training session on cybersecurity and public-opinion security, Li Zhe (李喆), a Qi An Xin engineer, gave presentations on the importance of information security, while Liu Chang (刘畅), the deputy general manager and editor-in-chief of *People's Daily Online*, discussed threats faced in cyberspace, including internet public opinion.[153]

Qi An Xin has worked closely with Sichuan Silence Information Technology—the cybersecurity company that Meta alleged was linked to the Facebook account of a fake Swiss biologist.[154] Under the guidance of the Cybersecurity Bureau of the MPS and sponsored by the Sichuan Provincial Public Security Department, Qi An Xin co-hosted the Sichuan Provincial Cybersecurity Level Protection System 2.0 National Standard Interpretation and Propaganda Conference (四川省网络安全等级保护制度2.0国家标准解读暨宣贯会) with Sichuan Silence Information Technology in November 2019 (Figure 20).[155]

Figure 20: Zhang Guanghua (张光华), party committee member and deputy director of the Sichuan Provincial Public Security Department speaking at the Sichuan Provincial Cybersecurity Level Protection System 2.0 National Standard Interpretation and Propaganda Conference

Source: Sichuan Silence Information Technology, archived.

Many of the Spamouflage-affiliated campaigns on US-based social-media platforms could be considered public-opinion guidance work, and there was some circumstantial evidence to suggest that Qi An Xin was affiliated with those types of cyber-enabled influence operations. For example, in the specific case of the Operation Honey Badger campaign conducted by Spamouflage network, inauthentic accounts directly amplified Qi An Xin Pangu Lab's report about NSA-linked activity on website forums,[156] which were then shared on Twitter.[157] Some posts by Spamouflage accounts used the distinctive logo of Qihoo 360 (a green plus symbol in the centre of a green and yellow pattern, which Qi An Xin also used while it was part of the 360 Group) in memes to suggest that Chinese cybersecurity companies were defending against NSA cyber operations (Figure 21). That was highly unusual, as Spamouflage networks had previously never used real Chinese corporate logos in their propaganda material. It's unclear why Spamouflage used the corporate logo in this campaign, but one possible theory is that it was to subconsciously promote Chinese cybersecurity companies.

Figure 21: An image shared by an account named ‘Renea’ using Qihoo 360’s distinctive green and yellow logo

Source: Twitter, archived.

Other Spamouflage accounts pulled content directly from Qi An Xin Pangu Lab’s report on allegedly NSA-related activity to disseminate propaganda about US cyber operations. In one case, a post by an inauthentic account named ‘News view’ appeared to be used by other accounts in the Spamouflage network as an anchor to reply to (Figure 22).[158] Similar tactics were used in previous pro-CCP inauthentic campaigns to create an appearance of organic engagement for other inauthentic accounts to avoid suspension and platform detection.[159] The text in the ‘News view’ tweet, however, confusingly referred to a different Qihoo 360 report named ‘The prelude to cyber warfare: the US National Security Agency (NSA) has launched indiscriminate attacks on the world for more than ten years’ (网络战序幕：美国国安局NSA对全球发起长达十余年无差别攻击), but the image shared under the post was clearly from page 16 of Qi An Xin Pangu Lab’s report.[160]

Figure 22: Screenshot of 'News view' post taken on 20 December 2022 with 461 replies but 0 likes and retweets

Source: Twitter, archived.

The image shared by 'News view' was interesting because it had a different layout from the original graphic in Qi An Xin Pangu Lab's report. The information depicted was unchanged, but the legend showing which industries were targeted was below the map, whereas in the original the legend was to the left of the map. The blue heading directly above the map was also new. In addition, the image shared by 'News view' appears to be a screenshot that's been hastily cropped. The right-hand side of the image has a dark border, and the whole image appears to be on a white background.

We could find similar images to the one 'News view' shared only in other Chinese state media articles, suggesting that this layout was specifically designed for propaganda purposes. For example, the WeChat account of 'Xinmin Weekly' (新民周刊, a magazine owned by the Shanghai United Media Group, which is overseen by the Shanghai CCP committee)[161] used a similarly formatted image but included information about which countries had been targeted.[162] Another article by Zhongguancun Blue Navy Civilian Integration Industry Promotion Association (中关村蓝海军民融合产业促进会), a military–civil fusion publication,[163] also used a similarly formatted and cropped image, but that article has now been deleted.[164]

Neither of the images used in those articles, however, had the same dark border on the right-hand side. One explanation could be that the image was a screenshot of the graphic when it was originally created by the authors of the Pangu Lab report before it was exported. If that was the case, then it would suggest a link between the inauthentic accounts on social media and Pangu Lab. Another explanation is that the operator controlling 'News view' had screenshot an image that had been imported into a word processor. This seems cumbersome when they could have just reshared the images that were already being disseminated by Chinese state media.

The evidence above might suggest that Qi An Xin is probably supporting the CCP's online influence operations by providing digital services to Chinese Government agencies controlling covert personas and creating material that's used in propaganda campaigns. Qi An Xin, directly and indirectly, benefits from the narratives disseminated by accounts in Operation Honey Badger identified in this report because that creates a demand for identifying and preventing US cyber operations, which Chinese cybersecurity services are currently offering. To become the world's number 1 cybersecurity company,[165] Qi An Xin will have to manage perceptions of its relationship with the Chinese state, which may be perceived as an espionage risk in potential international markets.[166] Narratives that claim that the US is also conducting cyberespionage campaigns undermine Western accusations that Beijing is conducting similar operations.

Qi An Xin's links to other influence operations

Like other Chinese enterprises, Qi An Xin's commercial activities are often aligned with the CCP's foreign policy interests. According to Wu Yunkun, the current CEO of Qi An Xin, the company exports its cybersecurity services overseas to protect Chinese companies such as Huawei and China Electronics Corporation in BRI countries.[167] Qi An Xin Pangu Lab won the Huawei Terminal Security Outstanding Contribution Award in 2019, and was the exclusive recipient of the 2020 Huawei Terminal Security Outstanding Contribution Award.[168] In 2020, Qi An Xin and Huawei CLOUD launched a mobile security service for government and enterprise employees to use virtual phones on the cloud.[169] Qi An Xin is one of China's 'hidden champions' (隐形冠军)—a company that isn't well known to the public but is developing core technologies that China lacks.[170] It takes that nomination literally, and steps have been taken to hide its affiliation with the internationally recognised Huawei. For example, Qi An Xin is listed on the Chinese-language version of Huawei's website as a terminal security partner,[171] but isn't listed on the equivalent English-language international version of the webpage.[172]

Qi An Xin's involvement with PLA military intelligence links adds further evidence to suggest that its claims of US cyber-espionage operations might be part of an influence operation. In 2019, Qi An Xin chairman, Qi Xiangdong, and Tomy Winata (aka Guo Shuofeng, 郭说锋), who is chairman of the Indonesian Artha Graha Network Group, signed an agreement at the Belt and Road Forum for International Cooperation to build a cyber threat awareness platform (Figure 23).[173] Tomy Winata is an Indonesian businessman who was apparently involved in Chinese military intelligence efforts to funnel money to the Democratic National Committee (DNC) for Bill Clinton's 1996 US presidential re-election campaign. According to a US Federal Bureau of Investigation report obtained by the *Los Angeles Times*, Winata sent Democratic fund-raiser Charlie Trie US$200,000 in travellers checks, a portion of which Trie used to make illegal contributions to the DNC.[174] Winata served as the main business partner of Lieutenant Colonel Liu Chaoying, an executive at China Aerospace International Holdings

and the daughter of former PLA General Liu Huaqing.[175] Liu Chaoying was working with Major General Ji Shengde, the former director of the PLA's General Staff Department (GSD) Intelligence Department (also known as the Second Department), who was responsible for PLA political influence operations.[176] According to Qi An Xin, the arrangement with Winata's Artha Graha Network Group was the first large-scale overseas cybersecurity infrastructure project launched by any Chinese cybersecurity company.[177] The CCP may perceive that agreement, and Winata's connections to both Indonesia and China, as an opportunity to build closer relationships with Indonesian political and military elites.[178]

Figure 23: Chairman of Artha Graha Network Group, Tomy Winata (AKA Guo Shuofeng) (left), and chairman of Qi An Xin, Qi Xiangdong (right), at the Second Belt and Road Forum for International Cooperation

Source: Qi Anxin, 'Direct attack on the "Belt and Road": Qi Anxin reached a cooperation with Indonesian AG Group', *Qianxin.com*, 25 April 2019, online (in Chinese).

Qi An Xin is also a key player in China's public technology diplomacy. A month after Pangu Lab's report on alleged NSA-linked APT activity was published in February 2022, Qi An Xin invited 20 military attachés from 18 Middle Eastern and African countries to show off the company's entire suite of cybersecurity products and services (Figure 24).[179] Qi An Xin boasted that it had developed the only system that's withstood the tests of 'actual cyber warfare' for the Beijing Winter Olympics, but that was probably a marketing angle. [180] The timing of Qi An Xin Pangu Lab's report suggests it was used to persuade the military and political elite in BRI countries that it offered sophisticated cybersecurity services that were even capable of detecting US cyber operations.

Figure 24: Defence attachés from 18 Middle Eastern and African countries visiting Qi An Xin

Source: 'Defense military attachés from eighteen countries visit QAX Group', QAX, 30 March 2022, online.

The Chinese Government's overt propaganda, clandestine CCP influence operations on social media and Qi An Xin's efforts to expand internationally are having an impact. In December 2021, Qi An Xin won a ¥70 million contract for APT monitoring in an unnamed country.[181] This announcement was published shortly after Qi Xiangdong attended and spoke at the APEC business leaders forum in Beijing.[182] Nearly a year later, Qi An Xin's subsidiary, Beijing Weiling Technology was awarded around US$20 million to build a cybersecurity centre, which included APT monitoring, in the capital of an unnamed country.[183]

There are several countries that could potentially be awarding Qi An Xin contracts for APT monitoring. According to Qi An Xin, it was involved in cybersecurity services in critical infrastructure for governments in Indonesia, Algeria, Angola and Ethiopia.[184] Indonesia is the only APEC country of those four. Qi An Xin CEO Wu Yunkun said the company had also entered the cybersecurity markets in Singapore and Canada at the 2022 World Internet Conference in Wuzhen, China.[185] Qi An Xin's terminal security partnership with Huawei suggests that it could be operating in any country that uses Huawei's telecommunications infrastructure. China's CAC, which often collaborates with the PLASSF and Qi An Xin in military–civil fusion cybersecurity initiatives,[186] has signed cybersecurity cooperation plans with Indonesia's National Cyber and Crypto Agency[187] and Thailand's National Cyber Security Agency.[188] Those will probably, if they don't already, involve cybersecurity expertise from Qi An Xin.

Hypothetically, if Qi An Xin were providing APT monitoring to the Indonesian Government, then the Chinese Government, by proxy through Qi An Xin, could seed disinformation directly to Indonesian cyber analysts to undermine regional relationships. Chinese Government-linked actors have already sought to shift the attribution of Chinese state-sponsored hacking group APT41 to the US Government.[189] Qi An Xin reports could likewise attribute cyber operations targeting Indonesian critical infrastructure originating from China to Australia or the US, which have been caught out spying on Indonesia and about which the Indonesian Government already harbours suspicion.[190]

The CCP's online influence objectives on social media

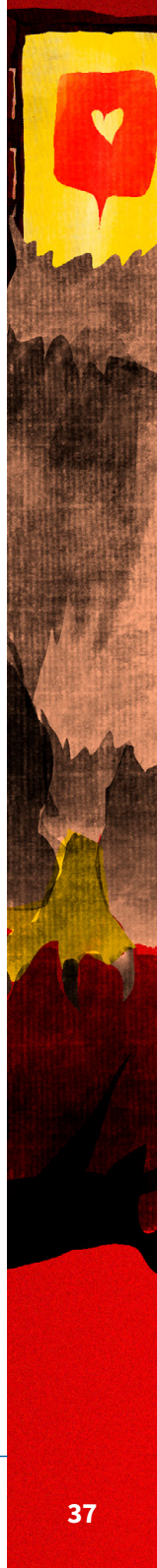
To understand CCP cyber-enabled influence operations, we must understand the CCP's broader objectives on social media. Chinese influence operations online are directly linked to the CCP's political security (政治安全).[191] The CCP remains paranoid that 'hostile forces' are using the internet to instigate 'colour' revolutions in China and destabilising the party's control. Only by increasing the CCP's position of power online and abroad can the CCP secure its legitimacy domestically.

Our review of Chinese agencies that have been suspected of employing covert personas on social media suggests that those operations are part of a broader strategy to shape global public opinion and enhance China's international discourse power. Researchers Nathan Beauchamp-Mustafaga and Michael S Chase proposed a framework for the PLA's use of social media based on Chinese academic sources in 2019.[192] The framework focused on PLA activities but, as is evident in the Operation Honey Badger case study above, covert Chinese influence operations could be conducted by the MPS, other Chinese party-state actors or by contractors on their behalf.

The CCP perceives the West as wielding disproportionate hegemony over China's right to set international agendas and undermining the effectiveness of its communications activities. US-based social media platforms such as Twitter and Facebook are still the preferred platforms for communications among international journalists, academics and activists. Western media outlets, such as the *New York Times*, the *Washington Post* or the British Broadcasting Corporation, are still perceived by global audiences to be more trusted and credible than Chinese state media.[193]

To compete against Western platforms such as Twitter and Facebook, the Chinese Government is supporting the overseas expansion of internet platforms that it has more control over, such as WeChat, TikTok and Kwai. By conducting covert influence operations on US-based social-media platforms that are easily detectable, the CCP could potentially be reinforcing negative news stories about those platforms in the press and pushing users to migrate to more 'entertaining' platforms, like TikTok.[194] Already, the Spamouflage network has previously sought to directly smear the Facebook brand and its founder Mark Zuckerberg in disinformation campaigns.[195] Key scenes for the contest will be in the emerging digital economies of the global South and Southeast Asia, where Chinese platforms are competitive.[196]

Covert accounts on social media also allow the CCP to pursue its interests while providing plausibly deniable cover. Since the beginning of the Covid-19 pandemic, international public perceptions of China have declined, and governments are responding negatively to Chinese diplomatic belligerence and human rights violations.[197] In response, the CCP has softened its public diplomacy, but it's true intentions can still be discerned in its clandestine operations. For example, the CCP covertly sought to undermine the emplacement of military bases in Japan's Okinawa Prefecture in 2022[198] and tried to impose costs on Western mining companies for threatening China's control over the global rare-earth supply chain by spreading disinformation about the companies to investors.[199] Those actions can be plausibly denied by the CCP and prevent countries such Australia and the US from raising these issues with international bodies such as the World Trade Organization.

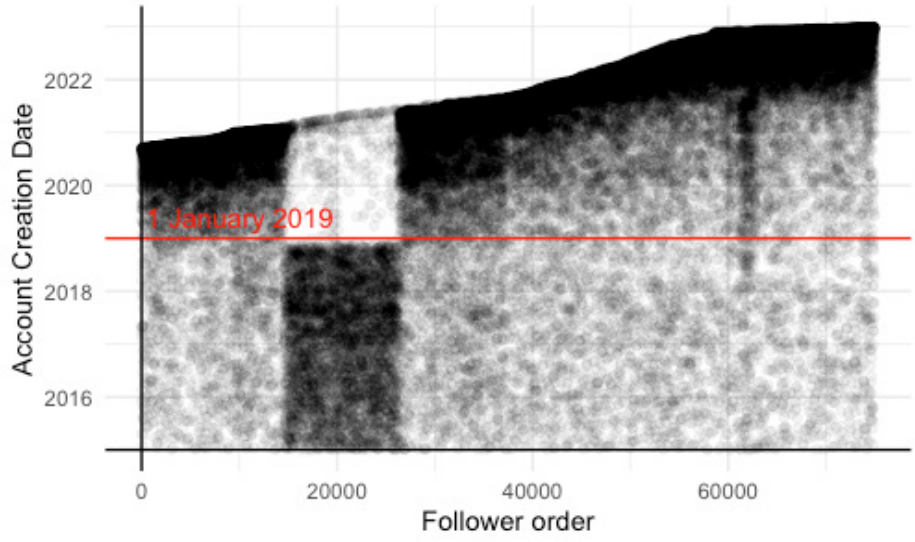


Emerging technologies and China's indigenous cybersecurity industry are creating new capabilities for the CCP to continue operating clandestinely on Western platforms. Chinese state-owned enterprises and private companies are playing an important role in China's future cybersecurity and threat awareness but are also possibly involved in offensive cyber operations. Influential Chinese scholars, such as He Haixiang, argue that the Chinese Government should invest in developing software to counter identity verification and algorithmic detection,[200] presumably to allow inauthentic personas to avoid suspensions. This includes the development of VPN channels, also known as 'green channels to the sea' (绿色出海通道), that hide the true origins of CCP operators.

From publicly available Chinese Government procurement documents, we suspect that the CCP is partly measuring the success of its cyber-enabled influence operations and propaganda based on online engagement metrics. That dependency on US-based social-media platform metrics is a weakness that counter-interference teams at social media companies and governments can exploit to prevent future online influence operations from improving.

For example, one bidding document, commissioned by the Propaganda Department of the Hangzhou Municipal Party Committee, asked vendors to increase the total number of followers of the 'Hangzhoufeel' Facebook, Twitter, Tuxing and YouTube accounts by 800,000 within a year.[201] The Hangzhoufeel Twitter account mostly posts positive depictions of Hangzhou city in China's Zhejiang Province but also posts tweets supportive of the Chinese Government's national policies and retweets official Twitter accounts affiliated with China's Ministry of Foreign Affairs.[202] As of January 2023, the Hangzhoufeel Twitter account had a little under 110,000 followers, but some of these accounts displayed coordinated inauthentic behaviour (Figure 25).[203] In 2021, the Hangzhoufeel account saw an influx of new followers created mostly before 2019, who mostly posted spam. This is unusual, since new Twitter followers tend to be created more closely to the date of an account that's then followed. These inauthentic accounts could potentially have been bought from a commercial spam network to boost the follower numbers. Inauthentically amplifying engagement with Hangzhoufeel may increase the perceived popularity of the account but it prevents the operators of Hangzhoufeel from understanding what content is in fact engaging with real users.

Figure 25: A density distribution plot of the most recent 75,000 Twitter followers of 'Hangzhoufeel' plotted by the account creation date and account follow order; darker regions show more accounts with similar creation dates



Source: ASPI analysis of Hangzhoufeel Twitter followers.

Policy recommendations

1. **Social-media platforms should take advantage of digital infrastructure, which they control, to more effectively deter cyber-enabled influence operations.**

   Well-funded and persistent adversarial actors appear to be innovating faster than the defence systems facing them. Rather than just defending against the inauthentic use of platforms, social-media platforms should neutralise the anticipated reward for the activity. In the case of online influence operations, that's often measured by engagement metrics, such as the number of impressions, followers or likes, which adversarial actors rely on for their internal impact assessments.

   To disrupt future influence operations, social-media platforms should remove access to those analytics for suspicious accounts breaching platform policies, making it difficult for identified malicious actors to measure the effectiveness of influence operations.

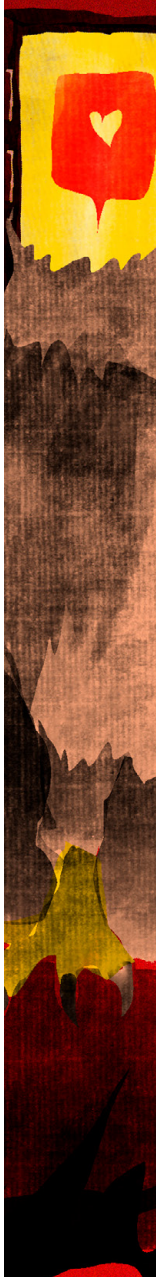
   Social media platforms could also consider a similar policy to address overt online influence operations and state propaganda. If, for example, an authoritarian state prevents its citizens from accessing Western platforms – which is the case in the PRC, North Korea and Iran – social media platforms could hide the engagement metrics of public social-media accounts affiliated with those authoritarian states until Western platforms are accessible again within those countries. This would deter states from artificially amplifying engagement on their posts, a common approach for well-resourced actors. It would also allow online users to assess propaganda posts based on content, rather than being led or influenced by the perceived popularity of the posts. Instagram has previously trialled similar policies to depressurise the platform, which was successful for some young people.[204]

2. **Social-media platforms should pursue more innovative information-sharing to combat cyber-enabled influence operations.**

   Social-media platforms have clear obligations to protect the privacy of their users. However, they also have room to review the type and volume of data they share with government agencies, civil society and other technology companies to combat cyber-enabled influence operations.

   The cybersecurity and advertising industries offer lessons on innovative ways to share data without breaching user privacy. For example, IP addresses and email addresses of known social-media accounts involved in online influence operations could be shared as hashed lists so that counter-influence-operation teams at other social-media platforms can compare assets to disrupt cross-platform campaigns. This would share information about digital assets that are involved in influence operations without revealing personally identifiable information.

   Social-media platforms should also work more closely with cloud computing companies such as Google, Amazon and Microsoft to disrupt the digital infrastructure (such as VPNs, cloud computing servers or compromised IoT devices) that are being used to disguise the origins of influence operations. Identifying and taking down these proxies would impose greater costs on malicious actors than just taking-down social-media accounts, blacklisting email address or phone numbers. Replacing and sustaining networks of devices or servers at scale to operate inauthentic



social-media accounts can be costly, whereas registering for new social-media accounts, email address or virtual phone numbers are often free or cheap to purchase. To support this new policy, researchers will have to shift the way they monitor foreign influence operations on social media, from analysing the narratives they disseminate to analysing the digital infrastructure malicious actors maintain to support those activities.

3. **Governments should consider social-media platforms to be critical infrastructure.**

   Social-media platforms are often disregarded as real spaces because they are intangible, but they form an important pillar of a nation's information ecosystem.[205] Those systems support information flows that are vital for the public to make informed decisions in a functioning democracy. Malicious actors already conceive of social-media platforms as a key means through which to influence publics and have increased their investment in offensive capabilities to attack this underprotected system within democracies. While social-media platforms might not be as critical as telecommunications or electricity grid infrastructure, policymakers should still consider policies and legislation that treat social-media platforms as a type of critical infrastructure.

   Governments should first change their language in speeches and policy documents to describe social-media platforms as critical infrastructure. This would acknowledge the existing importance of those platforms in democracies and would communicate signals to malicious actors that, like cyber operations on the power grid, efforts to interfere in the information ecosystem will be met with proportionate responses.

   In terms of regulation, voluntary codes such as the Australian Code of Practice on Disinformation and Misinformation, developed by the Digital Industry Group Inc., [206] are creative approaches to working with social-media platforms to counter online harms. However, if social-media platforms fail to meet the commitments in the code's objectives or if the code of practice appears to be ineffective in countering state-backed influence operations, then governments could legislate social-media platforms as a type of critical asset in critical infrastructure legislation, such as Australia's Security of Critical Infrastructure Act.[207] This would mandate regulatory requirements and administrative burdens on social-media platforms which may incentive them to fulfil their objectives set out in a voluntary code.

4. **Governments should review foreign interference legislation and consider mandating that social-media platforms disclose state-backed influence operations and other transparency reporting to increase the public's threat awareness.**

   Unlike traditional foreign interference and espionage, covert operations online can be difficult to attribute. Governments should consider mandating that social-media platforms disclose suspected state-backed influence operations and other transparency reporting to increase the public's threat awareness, either through voluntary codes of practice, such as the Australian Code of Practice on Disinformation and Misinformation, or through critical infrastructure legislation.

   This would require governments and social media platforms to develop agreed indicators and reporting thresholds. It would also require social media companies to reprioritise these issues and invest more resources, beefing up their counter-malign-influence teams. In return, governments could offer tax deductions (to a limited maximum amount) to incentivise social-media companies to maintain trust and safety teams that work on countering influence operations and other threats.

The ability of democratic governments to investigate influence operations on social media can also fall into a legislative gap between foreign interference and digital telecommunications services. Governments should review and update their foreign interference laws to address these new cyber-enabled threats.

For example, the Australian Government could consider proscribing social-media platforms as 'service providers' and allow 'exceptional access' authorisation to access the metadata of inauthentic accounts on social media. In Australia, the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* introduced offences for foreign interference that qualify as 'serious offences', as defined in section 5D of the *Telecommunications (Interception and Access) Act 1979*.[208] Furthermore, the *Australia-United States CLOUD Act* allows the Australian Government to request data from US-based technology companies to investigate serious crimes.[209]

As a baseline, authorisation to access social-media data should only be granted when it's both necessary and proportionate. Independent bodies should have strict oversight of these activities to prevent political misuse of those powers.

5. **Public diplomacy should be a pillar of any counter-malign-influence strategy.**

   Government leaders and diplomats should name and shame attributable malign cyber-enabled influence operations, and those entities involved in their operation (state and non-state), to deter those activities. Any public condemnation would require verifiable evidence to persuade other countries and may require declassifying intelligence to support claims in certain circumstances.

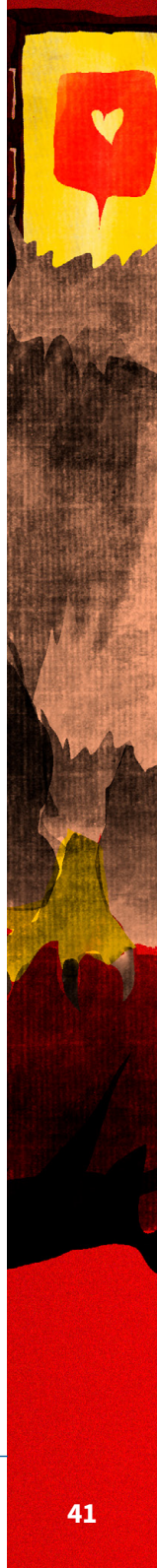
   Governments can both implement country-agnostic policies to counter cyber-enabled influence operations while also acknowledging that the CCP is a significant actor, the largest in the Indo-Pacific, and one that's increasing its capacity to manipulate online public opinion and perception through disinformation and influence operations. Public diplomacy and China-focused foreign policies should then play crucial roles in assuring and deterring the CCP from conducting these operations.

   Governments should also use their social-media accounts in China and domestically to highlight and push back against these operations. For example, the Japanese Government could use its social-media accounts to post messages exposing the actors and their tactics to spread disinformation about its bases in Okinawa.

6. **Partners and allies should strengthen intelligence diplomacy on this emerging security challenge and seek to share more intelligence with one another on such influence operations.**

   Strong open-source intelligence skills and collection capabilities are a crucial part of investigating and attributing these operations, the low classification of which, should making intelligence sharing easier.

   Governments or cybersecurity providers should also offer cybersecurity training to verify information, build capacity to identify technical disinformation and/or provide evidence-based assessments on state-sponsored activity.



7. **Governments should support further research on influence operations and other hybrid threats.**

   There are many aspects of cyber-enabled influence operations that are still unknown and contentious. Retrospective analysis of the impact of influence operations often misunderstands the intention, and hence measures the wrong effect, or relies on approximate measures of psychological impact. Cyber-enabled influence operations are also usually coordinated with other state actions, which makes it difficult to pinpoint their exact effects. Regardless, adversarial actors are heavily investing in their capabilities and are betting that future innovations will increase the impact of their operations.

   To build broader situational awareness of hybrid threats across the region, including malign influence operations, regional democracies should establish an Indo-Pacific hybrid threat centre (HTC).[210] This could be modelled on the NATO–EU Hybrid Centre of Excellence in Finland but would need to reflect the differences between the European and Indo-Pacific security environments. The HTC could be a decentralised model facilitating outreach across the region and would assist buy-in from ASEAN and the Pacific Islands Forum. Quad countries are well position to provide long-term commitments while other countries with experience and expertise in hybrid threats could provide additional support, particularly EU countries and the UK. Partnership arrangements with technology companies would provide technical insight and support.

   The research centre could also host 'influence operation ranges' where researchers can conduct experiments in controlled, interactive environments to test new tools, practice offence and defence, and understand future hybrid threat capabilities. These influence operations ranges could be modelled after cyber ranges.[211]

   The centre would build confidence through measures supporting research and analysis, greater regional engagement, information sharing and capacity building.

Appendixes

Appendix 1: Methodology and limitations

This project systematically collected and reviewed official and unofficial CCP propaganda narratives over a 12-month period and analysed the dissemination pathways of the CCP's increasingly advanced and adaptable information and disinformation apparatus. We also collected and reviewed a diverse range of publicly available information on CCP cyber-enabled influence operations, including:

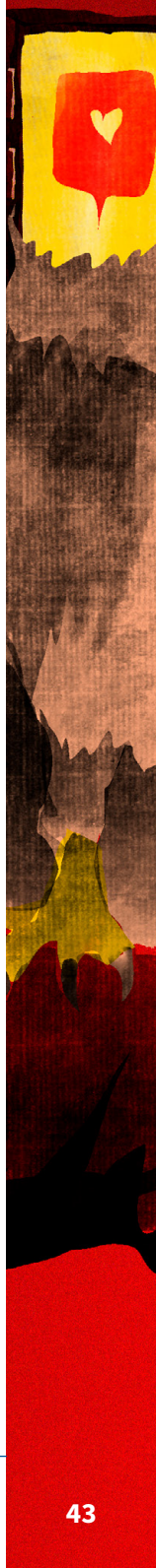
- Chinese Government documents, policy documents and procurement contracts
- Chinese academic literature
- previous reports on CCP cyber-enabled influence operations between 2017 and 2023
- takedown data disclosed by social-media companies between 2019 and 2023
- social-media posts by official Chinese diplomats and state media accounts on Twitter and Facebook
- social-media posts of accounts we assessed to be very likely to be affiliated with Spamouflage or other CCP cyber-enabled influence operations
- leaked government documents.

We compiled lists of China's Ministry of Foreign Affairs (MFA) spokespeople, diplomats, embassies and state media agencies and employees on US-based social-media platforms. Such lists have also been collated by the University of Oxford,[212] or are available on websites such as the Hamilton 2.0 Dashboard,[213] which is a project of the Alliance for Securing Democracy at the German Marshall Fund of the United States.

After identifying a new CCP propaganda campaign alleging that the US Government was conducting cyber operations, this project then collected data on those narratives across English- and Chinese-language social-media platforms. We used a combination of manual collection methods and social listening services offered by Meltwater. This data was then analysed by:

- Google Cloud computing services to store and manage the data
- qualitative assessments of capabilities and trends
- programming language R for data analysis and graph creation
- machine-learning algorithms to analyse images.

This project is limited by the quantity of publicly available information on covert activities. Our assessments of the trends in and capabilities of CCP influence operations relied on the integrity and exhaustiveness of previous publicly available reports. We believe that some CCP cyber-enabled influence operations have probably not been identified publicly due to more sophisticated persona creations or covert behaviour. This implies that our assessments of CCP capabilities are probably underestimates. There are also likely to be other pieces of information about these operations that we may have missed in the vast datasets disclosed by social-media platforms.

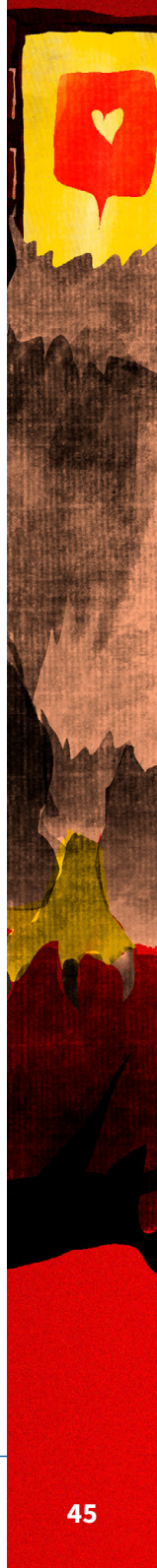


Appendix 2: Case history of CCP cyber-enabled influence operations

Table 2: Timeline of CCP-linked information operations from 2017 to 2022

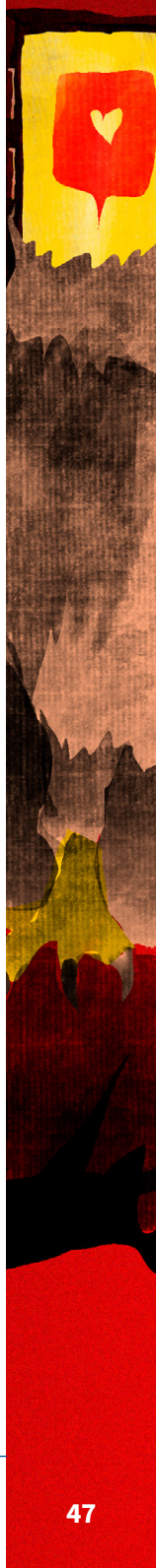
Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Oct 2017	The Daily Beast, online	Twitter	Guo Wengui (郭文贵, Miles Kwok)	Combination of coordinated trolls, probably automated	No attribution provided	Police
Aug 2019	Meta (Facebook), online 5 fake accounts, 7 pages, and 3 groups removed from platform	Facebook	Local political news, including Hong Kong protests	15,500 accounts followed one or more of the pages, and 2,200 accounts joined at least one of the groups (unable to identify authenticity of accounts)	Links to individuals associated with the Chinese Government	Police
	Twitter, online Disclosed 936 accounts (subset of a larger network of around 200,000 accounts)	Twitter	Hong Kong protests	Sophisticated and coordinated	Chinese state-backed	Police
	Google, online 210 channels removed	YouTube	Hong Kong protests	Coordinated	No attribution provided	Police
Sep 2019	ASPI, online Analysed three Twitter datasets	Twitter	Hong Kong protests Likely aimed at overseas Chinese audiences	Small and hastily assembled operation Accounts thought to have previously engaged in multiple information operations targeting Chinese Government's political opponents	Linked to the Chinese Government	Police
	Graphika, online First report of 'Spamouflage Dragon' ('Spamouflage')	YouTube, Twitter and Facebook	Hong Kong protests and Guo Wengui	Hijacked and fake accounts	Amplified state messaging but no attribution provided	Police
	IFTF's Digital Intelligence Lab, online	Twitter	Hong Kong protests and Taiwanese politics	Repurposed spam infrastructure, including bots and fake accounts, for political messaging	A high likelihood of belonging to the Chinese disinformation network that was removed	Political
Dec 2019	Taiwan Foundation for Democracy, online	Facebook	Taiwanese politics	A total of 88 other fan pages were found to be in the same 'community' that shared stories from a total of 117 template websites	Posts used 'officialized terms' used by *Xinhua News Agency*. Some fan pages didn't shy away from demonstrating the five-star flag and symbols and PLA symbols in their profile photos	Political
Mar 2020	*ProPublica*, online	Twitter	Covid-19, Hong Kong protests and other topics of interest to the Chinese state Chinese-language content	Engagement came from fake accounts	Spamouflage	Police/ Political

Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Apr 2020	Graphika, online	YouTube, Twitter and Facebook	Chinese regime critics, Hong Kong protests and Chinese response to Covid-19 Content in English and Chinese and hijacked accounts from Bangladesh	Some primary posters and some amplifier accounts Generated little engagement with authentic users	No attribution provided	Police/ Political
May 2020	Bellingcat, online Analysis of '#MilesGuo bot network'	Twitter and Facebook	Guo Wengui, Hong Kong protests, cryptocurrency, Elon Musk and Chinese response to Covid-19 Content in Chinese and other languages, including Russian	Newly created and stolen accounts	No attribution provided	Police/ Political
	BBC News, online 1,200 hijacked and automated social media accounts	YouTube, Twitter and Facebook	Chinese response to Covid, Hong Kong protests, Guo Wengui and US's handling of Covid	While the 53 Facebook pages had a combined following of 100,000 followers and YouTube accounts had 10,000 followers, most of the engagement across all platforms didn't come from authentic accounts	Displayed characteristics similar to Spamouflage and a Chinese state-backed information operation removed by Twitter and Facebook in 2019	Police/ Political
Jun 2020	ASPI, online	Twitter	Hong Kong protests	Unsophisticated	Some accounts had links to earlier campaigns that attacked the Chinese Government's political opponents Identified by Twitter and ASPI as Chinese state-backed	Police
	The Stanford Internet Observatory, online Twitter took down 23,750 accounts	Twitter	Hong Kong protests, Guo Wengui, with additional content centring on Covid-19 and a smaller subsection looking at Taiwan Posts in both Chinese and Russian languages	Personas weren't well developed Network failed to garner significant engagement	Linked to actor responsible for the August 2019 operation, emerging from the PRC	Police/ Political
	Twitter, online Disclosed 23,750 core accounts and 150,000 amplifier accounts	Twitter	Hong Kong protests and other Chinese geopolitical narratives Content in Mandarin and Cantonese	Coordinated but achieved poor engagement	Chinese state-backed	Police/ Foreign affairs



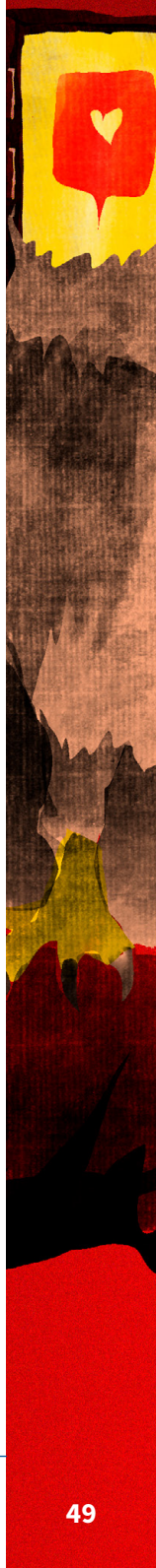
Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Aug 2020	Google, online Terminated 186 YouTube channels	YouTube	Largely non-political topics, with some focus on the US's response to Covid Content primarily in Chinese	Nil	No attribution provided	Political
	Graphika, online	Twitter, Facebook and YouTube	US foreign policy, US's handling of Covid, US racial inequalities and the US's crackdown on TikTok Included English-language content	AI-generated images were used in profiles and were highly reactionary to shifts in the US–China relationship	No attribution provided	Foreign affairs/ political
	Graphika, online 'Dracula's Botnet'	Twitter	US response to Covid, US racial discrimination and China–US relations Content in several languages, including Chinese, Korean and French	Probably commercial; unsophisticated and largely automated inauthentic accounts Didn't gain substantial following	Suspected as being part of the Spamouflage network	Political/ Foreign affairs
	Institute for Strategic Dialogue and Alliance for Securing Democracy, online	Twitter	Covid conspiracies, Taiwan independence, Taiwan's bid to join the WHO, Hong Kong protests and US racial discrimination protests Tweet replies targeted Donald Trump, Mike Pompeo, Tsai Ing-wen, media accounts of the *New York Times*, *Voice of America*, *Deutsche Welle*, the *BBC* and others Content in Chinese, English, Japanese and Urdu	Accounts were created between 10 am and 10 pm; tweeting occurred mainly between 10 am and 12 am (Beijing local time)	No attribution provided	Police/ Political
	Institute for The Future, Graphika, International Republican Institute, online	Facebook, Instagram, LINE, PTT, Twitter and YouTube	Taiwanese politics	The emergence of information operations involving Covid-19 makes it abundantly clear that disinformation in Taiwan is a persistent threat, not limited to election cycles	A range of links to mainland China, Chinese state media and pro-CCP content farms.	Political

Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Sep 2020	Graphika, online 'Operation Naval Gazing'	Facebook and Instagram	Dominant naval theme but also posted content on geopolitical themes from Taiwan and Hong Kong to Sino-US relations Content in Chinese, English, Filipino and Indonesian	Fake accounts, including new use of fake US accounts	Links to individuals in Fujian Province, China	Military / Foreign affairs
	Facebook, online Removed 155 accounts, 11 pages, 9 groups and 6 instagram accounts	Facebook and Instagram	Naval activity in the South China Sea Content in Chinese, Filipino and English, with the targets being the Philippines, Southeast Asia more broadly and the US	Audience engagement varied dramatically; no indication that engagement was from authentic accounts	No attribution provided Emerging from within the PRC	Military/ Foreign affairs
Oct 2020	Doublethink Lab, online More than 100 Facebook pages	YouTube, Facebook and Line	Taiwan's 2020 general election (anti-democracy) and Covid Content and subtitles in Chinese but attempts use Taiwanese terminology	Coordinated but ultimately low impact	'Patriotic and volunteer netizens from China'	Politics
Jan 2021	Graphika, online	Twitter	Belgian Government's plans to limit Chinese firms Huawei and ZTE's access to the country's 5G network	Didn't gain substantial traction other than amplification by real accounts of Huawei executives	No attribution provided	Technology
	Crime and Security Research Institute (Cardiff University), online Two-part report Network of 500 accounts (mix of authors and amplifiers)	Twitter	US politics (anti-Trump and anti-Biden) and Covid Content in Chinese; English posts machine translated	Operated as series of autonomous cells with minimal links; considered sophisticated and subtle with indication of the network trying to skirt detection Reactive to US events (amplified calls for violence before the Capitol riot and increased activity prior to the US election) Reached a wide audience and increased visibility of major media stories	'China-linked' Accounts active only during Chinese office hours Potential use of paid content farms	Political
Feb 2021	Graphika, online	Twitter, Facebook and YouTube	Guo Wengui, Hong Kong democracy, China, general anti-US and US–China relations	Growing in authenticity, with some accounts showing real attempts at persona development and reaching genuine users outside China	Increasingly entwined with Chinese state officials and state messaging	Foreign affairs / Political / Police



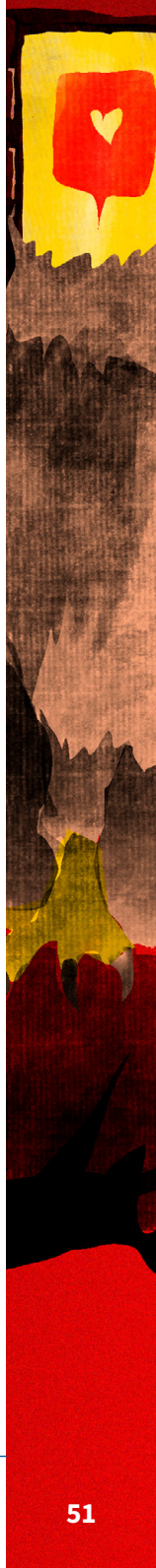
Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Apr 2021	Google, online Terminated 2,946 YouTube channels in Jan, 938 in Feb and 682 in Mar 2021	YouTube	US response to Covid, US domestic political divisions/social issues and China's Covid vaccine efforts Content in Chinese and English languages	Nil	No attribution provided	Political
May 2021	Oxford Internet Institute, online 62 accounts	Twitter	Amplified messaging of PRC diplomats stationed in the UK	Coordinated Drives a significant proportion of engagement with PRC UK-based diplomats	Many accounts were traced to a single person switching between multiple accounts in sequence	Foreign affairs
Jun 2021	*ProPublica* and the *New York Times*, online Thousands of videos emanating from Xinjiang	Local Chinese news platforms, YouTube and Twitter	Xinjiang and Mike Pompeo The Chinese- and Uyghur- language videos contained English subtitles	Videos didn't show signs of official propaganda but amplified state messaging, indicating a coordinated and sophisticated information operation	No attribution provided	Political
Jul 2021	*New York Times*, online 4,600 accounts	Twitter	Amplified PRC's messaging on Covid and other topics (undisclosed)	Some accounts retweeted at set time intervals, suggesting automation Accounts had very limited engagement	The users denied being part of a government campaign	Political
	ASPI, online	Facebook, Instagram, YouTube, Reddit. Google Groups, Medium, TikTok and a Russian amateur blog site	Asian racism, Dr Li-Meng Yan and the origins of Covid Targeting Chinese diaspora communities	Posted during Beijing business hours Use of multilanguage platforms indicates increased capability and coordination	Chinese state-linked	Political
Aug 2021	Centre for Information Resilience, online	Twitter, Facebook and YouTube .	US and Covid-19, US claims about human rights abuses in Xinjiang, US gun laws, US racial discrimination, US–India relations, Covid-19, Dr Li-Meng Yan, Guo Wengui, Hong Kong pro-democracy movement, US–China relations, US and global conflict and US and violence Content in Chinese and English languages	Coordinated attempt using real, fake and stolen accounts No measure of impact was provided	Amplified state messaging but no attribution provided	Political/ Police/ Foreign affairs

Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Sep 2021	Mandiant, online	30 social-media platforms and 40 additional websites and niche forums	Covid, Guo Wengui and the US's political issues Content in English, Chinese Russian, German, Spanish, Korean and Japanese	Use of AI-generated profile images, targeting of current events and activity on multiple platforms indicate an expanded online footprint and attempts at greater authenticity The network indicated intent to motivate real-world activity outside China	Dragonbridge	Police/ Political
Oct 2021	University of Oxford / *NBC News*, online Marcel Schliebs uncovered a network of more than 550 Twitter accounts	Twitter	Claimed that Covid-19 could have been imported to China from the US through a batch of Maine lobsters shipped to a seafood market in Wuhan in November 2019	Some of the accounts were 'unsophisticated sock puppets' with 'very few or zero followers', Schliebs said, while others appeared to be accounts that were once authentic but had been hijacked and repurposed to spread disinformation.	'Coordinated effort, and that it's a pro-Chinese narrative.'	Political
Dec 2021	ASPI, online	Twitter and Facebook	Xinjiang Targeted Chinese-speaking diaspora and international audiences with content in English and other non-Chinese languages	Coordination across the party-state's propaganda assets	Chinese state-linked	Political
	Meta, online Removed 524 Facebook accounts, 20 Pages 4 Groups and 86 Instagram accounts	Facebook	Hong Kong, Taiwan, US domestic politics, US foreign affairs and Covid Targeted audiences in the US, the UK, Taiwan, Hong Kong and Tibet	Several Chinese Government officials engaged with the content Considered to have had a negligible impact	Links to employees of information security firm Sichuan Silence Information Technology and individuals associated with Chinese state infrastructure companies	Political/ Foreign affairs
	ProPublica / *New York Times*, online Identified 97 fake accounts	Twitter	Promoting messaging about Peng Shuai from Hu, the *Global Times* editor, and other Chinese state media	Such accounts may have little traction, but they can help drown out critics and bolster friendly messages	Telltale signs that these and the hundreds of other analysed accounts were a part of campaigns to shape public opinion	Political
	Miburo, online 1,632 Facebook, 319 YouTube and 60 Twitter accounts	Facebook, Twitter and YouTube	Denying human rights abuses in Xinjiang, Taiwanese politics and cross-strait relations, Hong Kong protests, Guo Wengui, US–China relations and the US's Covid response Content in English, Chinese, Bengali, Turkish, Vietnamese and Arabic	Use of automated quotes from literature, AI-generated profile images and political ads Limited engagement outside network despite expanded messaging	Spamouflage	Police/ Forreign affairs



Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Feb 2022	*ProPublica* and the *New York Times*, online	Twitter	Beijing 2022 Winter Olympics	Used bots, fake accounts and real social-media influencers Little engagement outside network	'Spicy Panda' account is linked to iChongqing, a state-media-linked multimedia platform based in Chongqing	Political
Apr 2022	Institute for Strategic Dialogue, online 'Pro-CCP network' (Spamouflage)	Twitter	Amplified Russia's state messaging on Ukraine Content in English with English and Chinese subtitles	Coordinated activity (use of stock image profile pictures, similar bios, batch account creation, username and profile picture inconsistencies, synchronised comments and retweeting and activity within Beijing business hours) Failed to gain traction with authentic users	Part of Pro-CCP network (Spamouflage)	Military
	ASPI, online A pro-CCP network of at least 80 accounts across Western social media	Twitter, Facebook, Reddit and YouTube	Japan's military activities and the Quad Content in German, Spanish, French, English and Chinese	Poorly operated (errors in hashtags, incomplete URLs, evidence of instructions posted in tweets), indicating coordination and possible automation Accounts posed as citizens in Australia, India, Japan and the US Ultimately low impact	Spamouflage	Military/ Foreign affairs
	Institute for Strategic Dialogue, online 33 hijacked accounts	Twitter	Russo-Ukrainian war; Kazakhstan and 'colour revolutions'; US domestic policy and internal relations Content in French, English and Mandarin	Hijacked accounts included those of French MP Bernard Reynès and Spanish politician Liliana Pérez Pazo Accounts were active during Beijing working hours; followership of accounts was inauthentic	Spamouflage	Military/ Political

Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Jun 2022	ASPI, online	Twitter	Targeting smart Asian women Content in English and Mandarin	Accounts used either images of real women or AI-generated images as profile pictures; accounts were active during Beijing business hours	Spamouflage	Abuse
	Mandiant, online	Twitter and Facebook	Smearing rare-earth mining companies from Australia, Canada and the US Content in English and Chinese	Leveraged commentary by real people (some accounts posed as residents of Texas) Considered only partially effective with limited engagement from real individuals	Dragonbridge	Military
	ASPI, online	Facebook, Instagram and Twitter	Undermining rare-earth supply-chain diversification, including by smearing Australian company Lynas Rare Earths and the Western Australian Government Intended to reach audiences in the US, Australia and Malaysia	Accounts posed as Western women Some accounts engaged with apparently real individuals, but interaction with content was low across all platforms	Spamouflage	Military
Aug 2022	Mandiant, online A network of at least 72 suspected inauthentic news sites and a number of suspected inauthentic social media assets	Websites, Facebook and Twitter	Criticising the US and its allies; attempting to reshape the international image of Xinjiang due to mounting international scrutiny; expressing support for the reform of Hong Kong's electoral system (a change that gave the PRC more power over vetting local candidates)	Some evidence to suggest that 'HaiEnergy' failed to generate substantial engagement outside of inauthentic amplification	Aligned with the political interests of the PRC	Political



Date	Source / summary	Platform	Narrative / target audience	Sophistication / impact	Attribution	Category
Oct 2022	ASPI, online	YouTube, Twitter and Facebook	Obscuring human rights abuses in Xinjiang Targeting audiences outside China	Use of popular Uyghur, Kazakh and other minority social-media influencers to parrot Chinese-state messaging in a more subtle way than traditional propaganda Accounts garnered a significant audience with millions of followers	Linked to influencer-management agencies multichannel networks) Chinese state-linked	Political
	Mandiant, online	Twitter	Claims that China-nexus APT41 is a US Government-backed actor; discrediting US democratic processes; accusations that the US was responsible for the Nord Stream gas-pipeline explosions English and Chinese content targeting US citizens	Accounts posed as Americans and plagiarised news media articles Operation had limited impact	Dragonbridge	Political/ Military
	Alethea Group, online 165 Twitter accounts	Twitter	Posted politically polarising content related to the 2022 US midterm elections	Number of accounts identified is relatively small and they received very little engagement	Spamouflage	Political/ Military
Nov 2022	Election Integrity Partnership, online Six distinct authentic networks	Twitter	US 2022 midterms (political opinions regarding Taiwan and stance towards China)	Networks made to appear as if they were operating from within the US The network had limited engagement with online public	Links to China	Political
	ASPI, online	Twitter	Targeting smart Asian women	Increased intensity of network's activity	Spamouflage	Abuse

Appendix 3: Possible Spamouflage linkages to APT41

On 26 September 2022, to investigate the underlying network infrastructure of Spamouflage-affiliated accounts, we sent 'canary tokens' to six Reddit accounts that were highly likely to be involved in Operation Honey Badger. Canary tokens can be files, links or other digital resources that are monitored for access.[214] In our case, we sent URL links that recorded the IP addresses of devices accessing the link. Between 16 and 19 November 2022, those canary tokens were activated by 24 unique IP addresses (see Table 3). Almost all the IP addresses identified belonged to virtual proxy networks and had been reported for network abuse. One IP address (185.220.101.37) had been detected by the UK-based cybersecurity firm, Security Blue Team, for conducting log4j vulnerability identification scanning and exploitation in December 2021, a month after the vulnerability was discovered.[215] That IP address is listed as a Tor Exit node but had low traffic volume, indicating that it was reserved for one

actor. Cybersecurity firm Mandiant previously reported in May 2021 that the log4j vulnerability was being exploited by APT41, which is a Chinese state-sponsored APT actor linked to the MSS, to target US state governments.[216] We couldn't verify whether the IP address was linked to APT41.

The discovery of an asset exploiting the log4j vulnerabilities adds to a growing body of evidence suggesting a possible nexus between Chinese state-sponsored hackers and the Spamouflage network. In December 2022, the US Secret Service accused APT41 of stealing at least $20 million in US Government coronavirus relief funds.[217] APT41's efforts to steal Covid-19 relief funds appeared to be financially motivated but could also have supported a broader political warfare campaign to foment discontent about US Government officials among US taxpayers. Earlier in 2022, accounts probably linked to the Spamouflage network were amplifying claims of US officials misappropriating Covid-19 relief funds[218] and falsely claimed that 'all kinds of defence cooperative enterprises, government officials, and even the Ministry of National Defense and the Ministry of Health were embezzling anti-epidemic funds.'[219]

As part of Operation Honey Badger, Spamouflage-linked accounts appeared to repurpose legitimate reporting about APT41 to blame Chinese cyber-espionage operations on the US Government instead. A *TechCrunch* article published in March 2022 was edited and redistributed on multiple social-media platforms and forums.[220] The original article began with the statement:

> The prolific China APT41 hacking group, known for carrying out espionage in parallel with financially motivated operations, has compromised multiple US state government networks, according to cybersecurity giant Mandiant.

Accounts linked to the Spamouflage network replaced key entities so that the article instead read:

> The prolific US-backed APT41 hacking group, known for carrying out espionage in parallel with financially motivated operations, has compromised multiple Russian state government networks, according to a Chinese cyber security enterprise Qi An Xin Technology Group Inc.[221]

In October 2022, Spamouflage accounts flooded the #APT41 hashtag on Twitter with posts accusing the US Government of cyber-espionage operations and burying other posts about APT41.[222] More than 400 Twitter accounts impersonating Intrusion Truth's Twitter account were also created in October.[223] This was a common tactic deployed by Spamouflage-affiliated networks to divert online attention away from accounts unfavourable to the CCP and has been used to target smart women of Asian descent.[224]

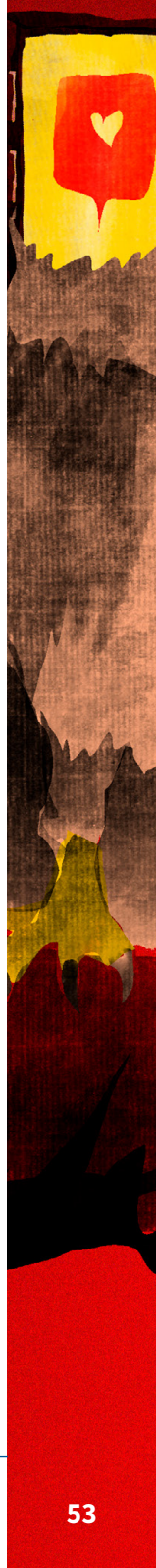


Figure 26: Spamouflage accounts spreading disinformation about APT41

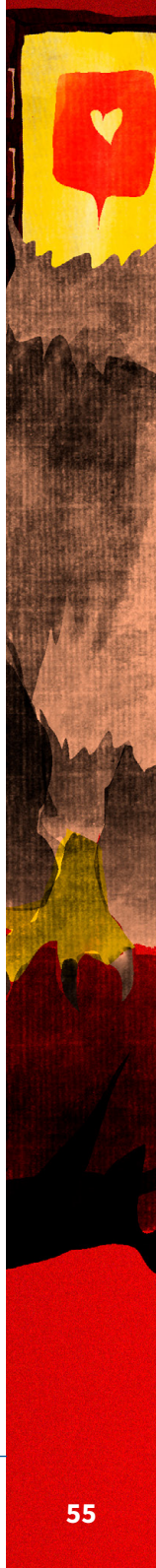
Source: Twitter (left, online), (right, online).

Taiwanese cybersecurity company TeamT5 previously warned about the combination of APT actors and influence operations as a concerning development in Chinese information operations targeting global audiences.[225] TeamT5 uncovered evidence of Chinese APT actors disseminating disinformation on the PTT Bulletin Board System (批踢踢實業坊), which is an online forum popular in Taiwan. Accounts on PTT had been compromised to post alleged confidential information related to the Taiwanese Government.

Table 3: IP addresses triggering canary tokens sent to Spamouflage-linked accounts

IP addresses	Date triggered	User agent details	Who is lookup	Country of origin
35.203.245.221	2022–11–15 22:58:57 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.55 Safari/537.36 Edg/96.0.1054.43	GOOGLE-CLOUD	US
147.147.220.88	2022–11–15 23:20:55 (UTC)	Mozilla/5.0 (iPhone; CPU iPhone OS 16_0_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.0 Mobile/15E148 Safari/604.1	Plusnet	UK
92.17.141.4	2022–11–15 23:19:26 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36	Carphone Warehouse Broadband Services	UK
169.53.184.173	2022–11–16 00:00:05 (UTC)	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0	SoftLayer Technologies, Inc.	US
95.25.71.39	2022–11–16 00:02:19 (UTC)	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)	CORBINA TELECOM Network Operations	Russia
204.101.161.19	2022–11–16 00:03:33 (UTC)	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36	Bell Canada (LINX)	Canada
149.19.252.219	2022–11–16 00:06:39 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36	OCULUS NETWORKS INC	US
185.181.115.176	2022–11–16 00:09:15 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36	Ibraheem Massalha	Germany

IP addresses	Date triggered	User agent details	Who is lookup	Country of origin
45.79.42.132	2022–11–16 00:11:07 (UTC)	Spider_Bot/3.0	LINODE-US	US
193.128.111.42	2022–11–16 00:14:23 (UTC)	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_8; en-US) AppleWebKit/532.5 (KHTML, like Gecko) Chrome/4.0.249.0 Safari/532.5	Verizon Business Special Project	UK
35.203.245.186	2022–11–16 01:04:47 (UTC)	Mozilla/5.0 (Linux; Android 10) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Focus/1.0 Chrome/59.0.3029.83 Mobile Safari/537.36	GOOGLE-CLOUD	US
185.220.101.37	2022–11–16 01:06:50 (UTC)	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)	Network for Tor-Exit traffic	Germany
52.17.54.30	2022–11–16 01:14:29 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.75 Safari/537.36	Amazon Technologies Inc.	Ireland
206.189.247.132	2022–11–16 01:35:34 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36	DigitalOcean, LLC	UK
35.86.147.173	2022–11–16 02:08:10 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36	Amazon Technologies Inc.	US
185.183.106.155	2022–11–16 02:10:29 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36	GLOBALAXS NOC	Spain
52.17.54.30	2022–11–16 03:33:25 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.75 Safari/537.36	Amazon Technologies Inc.	Ireland
115.89.74.126	2022–11–16 11:15:25 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36	LG DACOM Corporation	South Korea
23.128.248.20	2022–11–16 12:29:20 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36	StormyCloud Inc	US
195.123.241.30	2022–11–16 18:10:29 (UTC)	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36	Green Floid LLC	US
205.169.39.255	2022–11–17 00:41:21 (UTC)	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36	CenturyLink Communications, LLC	US
52.116.65.37	2022–11–18 09:10:04 (UTC)	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0	SoftLayer Technologies Inc.	US
35.192.33.162	2022–11–18 12:04:29 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75 Safari/537.36	GOOGLE-CLOUD	US
209.170.91.202	2022–11–19 11:05:09 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75 Safari/537.36	TELIANET-2BLK	US



Appendix 4: Qi An Xin (奇安信)

Qi An Xin is a Chinese cybersecurity company founded by Qi Xiangdong in 2015 as the corporate-technology subsidiary of Qihoo 360 Technology—one of China's biggest internet security firms, which Qi co-founded with Zhou Hongyi (Figure 27).[226]

Figure 27: Qi Xiangdong and Wu Yunkun in front of Qi An Xin employees

Source: Qi An Xin Group Corporate Social Responsibility Report.

Prior to 2019, Qi An Xin was known as 360 Enterprise Security (360企业安全) before the company separated from the 360 Group. Western analysts and researchers commonly misattributed Qi An Xin's relationships with Chinese military and security agencies to Qihoo 360, since they once shared similar logos and names (Figure 28).

Figure 28: Logos associated with Qi An Xin

Qi An Xin's links with the Chinese party-state

Qi An Xin's party committee, which is subordinate to the party committee of the Beijing Internet Association (首都互联网协会), was formed in December 2018, according to the company's 2021 annual report.[227] The company has more than 1,300 CCP members (14% of its employees). Over 40% of its main revenue comes from government and law-enforcement agencies, and its clients also include users from the military and the defence industry.[228] The following outlines Qi An Xin's other party-state links but isn't intended to be an exhaustive list.

Some of Qi An Xin's shareholders have state ties:

- China Electronics Corporation (CEC) Capital Investment Holdings Company Limited (中电金投控股有限公司), holds 2.3% of Qi An Xin's shares, and Ningbo Meishan Bonded Port Area Mingluo Investment Management Partnership (Limited Partnership) (宁波梅山保税港区明洛投资管理合伙企业 (有限合伙) holds 17.88%.[229] CEC Capital Investment Holdings is a wholly owned subsidiary of CEC. It's also a partner of another Qi An Xin shareholder, Ningbo Meishan Bonded Port Area Mingluo Investment Management Partnership (Limited Partnership) (宁波梅山保税港区明洛投资管理合伙企业 (有限合伙)), which is majority-owned (99%) by CEC through CEC Capital Investment Holdings. CEC is also a shareholder of China's National Military & Civil Integration Industrial Investment Fund (国家军民融合产业投资基金).[230] CEC is ranked very high risk by ASPI's *China Defence Universities Tracker* for being one of China's leading producers of military electronics.[231] The company was added to the Non-SDN Chinese Military–Industrial Complex Companies List by the US Government's Office of Foreign Assets Control in March 2021.[232]
- Beijing Financial Street Capital Operation Group Co. Ltd (北京金融街资本运营集团有限公司), holds 3.55% of Qi An Xin's shares.[233] The group is wholly owned by the Beijing Xicheng District branch of the State-owned Assets Supervision and Administration Commission (北京市西城区人民政府国有资产监督管理委员会).[234]
- Hexie Chengzhang Phase II (Yiwu) Investment Centre (Limited Partnership) (和谐成长二期(义乌)投资中心 (有限合伙)), holds 1.68% of Qi An Xin's shares.[235] The largest shareholder (35.64%) of Hexie Chengzhang is the National Council for Social Security Fund of the PRC (全国社会保障基金理事会).[236]

Qi An Xin has direct and indirect working relationships with the MPS:

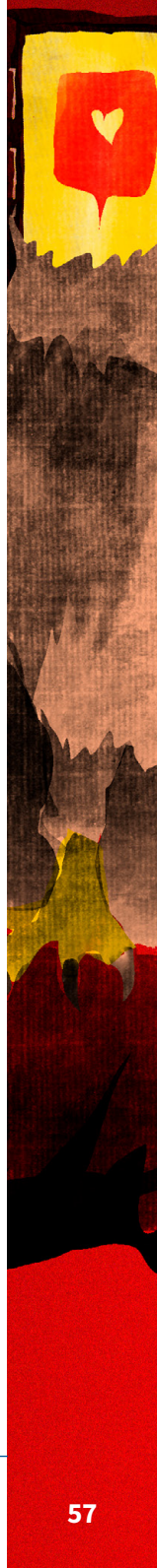
- The MPS sent a letter of thanks to Qi-Anxin Group in recognition of Qi An Xin's positive contribution to supporting network security protection in the MPS's 2021 special cybersecurity campaign.[237]
- In 2020, Qi An Xin signed a strategic cooperation agreement with the MPS's Third Research Institute (公安部第三研究所) to jointly work on a range of topics, including the development of cybersecurity products and setting national and industrial standards.[238]
- Qi An Xi built the Comprehensive Security Management Platform for the MPS, according to the website of Qi An Xin (Hong Kong).[239]

Qi An Xin has direct and indirect working relationships with the MSS:

- Qi An Xin subsidiary Wangshen Information Technology (Beijing) Co. Ltd (网神信息技术 (北京) 股份有限公司) is an authorised training institution appointed by the MSS's 13th Bureau's China Information Technology Security Evaluation Centre (CNITSEC, 中国信息安全测评中心)[240] according to the website of Qi An Xin (Hong Kong).[241]
- Qi An Xin and CNITSEC jointly established the CISP Cyber Security Penetration Testing Centre (攻防领域考试中心).[242]

Qi An Xin is involved in military–civil fusion:

- Qi An Xin is a vice corporate president of the Zhongguancun Science and Technology Innovation Smart Military Industry Technology Innovation Strategic Alliance (中关村科创智慧军工产业技术创新战略联盟), which was launched by nine institutions, including the Information Centre of the State Administration for Science Technology and Industry for National Defence (国家国防科技工业局信息中心) in 2017.[243]



- According to a 2022 job vacancy advertisement, Qi An Xin engineers are expected to build a technical team to serve military clients.[244]
- Qi Xiangdong and 360 Enterprise Security Group established the Cyberspace Security Military–Civil Integration Innovation Center in 2017.[245]

Qi Xiangdong (齐向东), founder and chairman of Qi An Xin

Figure 29: Qi Xiangdong

Qi Xiangdong, former deputy director of the Communication Bureau of Xinhua News Agency is the founder, chairman, largest shareholder[246] and party secretary of Qi An Xin. He has been bestowed the title of 'Outstanding secretary of the party organisation of the Party Committee of the Capital Internet Association (首都互联网协会党委优秀党组织书记).'[247]

In addition, Qi has held positions in several municipal- and national level united front organisations:[248]

- member of the 14th National Committee of the Chinese People's Political Consultative Conference (CPPCC)[249]
- member of the CPPCC[250] Beijing Municipal Committee
- executive member, All-China Federation of Industry and Commerce (全国工商联)[251]
- vice president, Beijing Federation of Industry & Commerce (北京市工商联)
- member of Big Data Operation and Maintenance (Network Security) Committee (大数据运维 (网络安全) 委员会) of the All-China Federation of Industry and Commerce (中华全国工商业联合会).[252]

Qi Xiangdong has also held senior positions in some government-controlled entities:[253]

- external director of Beijing Municipal People's Government State-owned Assets Supervision and Administration Commission (北京市人民政府国有资产监督管理委员会)
- vice president, China Confidentiality Association (中国保密协会)[254]
- vice president, Cyber Security Association of China (中国网络空间安全协会)[255]
- vice president, Internet Society of China (ISC, 中国互联网协会)[256]
- director, National Engineering Laboratory for Big Data Collaborative Security Technology (大数据协同安全技术国家工程实验室).[257]

Wu Yunkun (吴云坤), chief executive officer (CEO) of Qi An Xin

Figure 30: Wu Yunkun

The other person of significance at Qi An Xin is its CEO, Wu Yunkun. Wu completed his master's degree at the Nanjing University of Aeronautics and Astronautics in 2000.[258] He was president of 360 Enterprise Security Group.[259] Wu has also held positions in government-linked entities, including:[260]

- vice president, Informatisation Promotion Working Committee, China Information Industry Association (中国信息协会信息化促进工作委员会副会长)[261]
- deputy director, Cyber Security Committee, National Internet Finance Association of China (中国互联网金融协会网络与安全专委会副主任委员)
- member of an expert committee, People's Daily Smart Media Institute (人民日报智慧媒体研究院专家委员会委员)
- expert committee member, Cyberspace Security and Rule of Law Collaborative Innovation Centre, People's Public Security University of China (中国人民公安大学网络空间安全与法治协同创新中心专家组专家)[262]
- member of the first information system security protection technology professional group of the Equipment Development Department of the Central Military Commission.[263]

Notes

1 Nathaniel Gleicher, 'Coordinated inauthentic behaviour explained', Meta, 6 December 2018, online.

2 Jacob Wallis, Albert Zhang, *Understanding global disinformation and information operations: insights from ASPI's new analytic website*, ASPI, Canberra, 30 March 2022, online.

3 Nathan Beauchamp-Mustafaga, 'Cognitive domain operations: the PLA's new holistic concept for influence operations', *China Brief*, 6 September 2019, online.

4 Peter Mattis, 'China's three warfares in perspective', *War on the Rocks*, 30 January 2018, online.

5 Qi An Xin is also referred to as QAX Technology Group Inc. on the English version of its official site: online.

6 Fergus Ryan, Ariel Bogle, Nathan Ruser, Albert Zhang, Daria Impiombato, *Borrowing mouths to speak on Xinjiang*, ASPI, Canberra, 10 December 2021, online; Stella Chen, 'Discourse power', *China Media Project,* 30 May 2022, online; Renee DiResta, Carly Miller, Vanessa Molter, John Pomfret, Glenn Tiffert, *Telling China's story: the Chinese Communist Party's campaign to shape global narratives*, Stanford Internet Observatory and the Freeman Spogli Institute for International Studies, 20 July 2020, online; Toni Freidman, *Lexicon: 'Discourse power' or the 'right to speak' (话语权, Huàyǔ Quán)*, DigiChina Stanford University, 17 March 2022, online.

7 Louisa Lim, Julia Bergin, 'Inside China's audacious global propaganda campaign', *The Guardian*, 7 December 2018, online.

8 Ryan et al., *Borrowing mouths to speak on Xinjiang*; Fergus Ryan, Daria Impiombato, Hsi-Ting Pai, *Frontier influencers: the new face of China's propaganda*, ASPI, Canberra, 20 October 2022, online.

9 Nadege Rolland, *China's vision for a new world order*, National Bureau of Asian Research, 2020, online.

10 Such as ASPI, the Stanford Internet Observatory and private company Graphika.

11 In October 2022, a likely Spamouflage-linked campaign sought to bury Safeguard Defender's latest report on Chinese transnational policing. Accounts on TikTok were clearly involved in this campaign. See Albert Zhang's Twitter thread, online.

12 This network was probably initially reported by the *Daily Beast*: Ben Collins, Joseph Cox, 'This Twitter bot army is chasing down a Chinese dissident and Mar-a-Lago member', *The Daily Beast*, 27 October 2017, online. ASPI's analysis of the networks disclosed by Twitter found that they were active from April 2017: Tom Uren, Elise Thomas, Jacob Wallis, *Tweeting through the Great Firewall*, ASPI, Canberra, 3 September 2019, online.

13 Ben Nimmo, C Shawn Eib, L Tamora, 'Cross-platform spam network targeted Hong Kong protests', Graphika, 2019, online.

14 'Pro-PRC DRAGONBRIDGE influence campaign targets rare earths mining companies in attempt to thwart rivalry to PRC market dominance', *Mandiant Threat Intelligence*, 2022, online.

15 Uren et al., *Tweeting through the Great Firewall*.

16 'Information operations directed at Hong Kong', *Twitter Safety*, 19 August 2019, online.

17 Nathaniel Gleicher, 'Removing coordinated inauthentic behavior from China', Meta, 19 August 2019, online.

18 Marianna Spring, 'Twitter insiders: We can't protect users from trolling under Musk', *BBC News*, 6 March 2023, online.

19 Ben Nimmo, David Agranovich, 'Removing coordinated inauthentic behavior from China and Russia', Meta, 27 September 2022, online.

20 This report didn't reveal a new campaign but was a review of Spamouflage/Dragonbridge-related activity over 2022: Zak Butler, Jonas Taege, 'Over 50,000 instances of DRAGONBRIDGE activity disrupted in 2022', Threat Analysis Group, 26 January 2023, online.

21 Renée Diresta, Carly Miller, Vanessa Molter, John Pomfret, Glenn Tiffret, *Telling China's story: The Chinese Communist Party's campaign to shape global narratives,* Stanford Internet Observatory and the Hoover Institution, 2020, online; Albert Zhang, '#StopAsianHate: Chinese diaspora targeted by CCP disinformation campaign', *The Strategist*, 1 July 2021, online.

22 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'.

23 Danielle Cave, Albert Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women', *The Strategist*, 6 November 2022, online; see ASPI's 'Submission to the Senate Select Committee on Foreign Interference through Social Media', Australian Parliament, 22 February 2023, online.

24 Cave & Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women'; see ASPI's 'Submission to the Senate Select Committee on Foreign Interference through Social Media'.

25 See archive of Twitter account, online.

26 'Hundreds of fake Twitter accounts linked to China sowed disinformation prior to the US election—report', news release, Cardiff University, 28 January 2021, online.

27 Albert Zhang, Danielle Cave, 'Smart Asian women are the new targets of CCP global online repression', *The Strategist*, 3 June 2022, online; Cave & Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women'.

28 Amelia Loi, Mary Zhao, 'For female journalists, covering China comes at a cost', *Radio Free Asia*, 20 March 2023, online; Dorothy Wickenden, 'Jiayang Fan on navigating her mother's illness while becoming a target for Chinese nationalists online', *The New Yorker*, 10 September 2020, online.

29 Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi, Ido Wulkan, *AI and the future of disinformation campaigns*, Center for Security and Emerging Technologies, December 2021, online; Josh A Goldstein, Girish Sastry, Micah Musser, Renee DiResta, Matthew Gentzel, Katerina Sedova, 'Forecasting potential misuses of language models for disinformation campaigns and how to reduce risk', *OpenAI*, 11 January 2023, online.

30 On Monday 17 April 2023, the US DOJ unsealed a complaint alleging 34 Ministry of Public Security (MPS) officers 'created thousands of fake online personas on social media sites, including Twitter, to target Chinese dissidents through online harassment and threats'

as part of an elite task force named the '912 Special Project Working Group'. Those officers were possibly operating some of the personas in the network popularly known as Spamouflage, which ASPI has tracked since Twitter and Meta attributed it to the Chinese government in 2019: '40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents', US Department of Justice, 17 April 2023, online.

31 See screenshots in Albert Zhang, 'Pro-CCP inauthentic social media accounts shift focus to the Quad', *The Strategist*, 19 April 2022, online; see archived tweet.

32 This method speeds up the image-creation process and also removes metadata created in image exports. See Figure 30 in Jacob Wallis, Tom Uren, Elise Thomas, Albert Zhang, Samantha Hoffman, Lin Li, Alexandra Pascoe, Danielle Cave, *Retweeting through the Great Firewall*, ASPI, Canberra, 12 June 2020, online.

33 See Albert Zhang's Twitter thread, online.

34 Nathan Beauchamp-Mustafaga, Michael S Chase, *Borrowing a boat out to sea: the Chinese military's use of social media for influence operations*, Johns Hopkins School of Advanced International Studies, Foreign Policy Institute, 2019, online.

35 The October 2022 release of data by Twitter showed that accounts were being created from the PRC, Hong Kong and the US. See the latest Twitter October release on APAC 3; locations include the US, Hong Kong, Singapore and the PRC.

36 'Twitter accounts of European politicians hijacked to spread CCP propaganda', Institute for Strategic Dialogue, 22 April 2022, online.

37 Jeff Kao, Mia Shuang Li, 'How China built a Twitter propaganda machine then let it loose on coronavirus', *ProPublica*, 26 March 2020, online. According to threat intelligence company, Nisos, OneSight had also developed a sophisticated social-media management and monitoring system to propagate political disinformation against the Uyghur community: 'Chinese commercial firm OneSight conducts disinformation operations in support of the Chinese state against Uyghurs', Nisos, 23 November 2021, online.

38 *ProPublica* identified a handful of accounts boosting OneSight's social media marketing posts. OneSight also held a contract to boost the Twitter following of *China News Service*, which is a media organisation under the United Front Work Department. OneSight was later hacked by an anonymous group, CCP Unmasked, in 2020. According to Clint Watts, companies such as Onesight (一网互通), Nothing Technologies (无为科技), Urun Big Data Services (云润大数据服务), Chinaii (中国网络情报中心), and others, have also assisted in the government's censorship and propaganda campaigns: Clint Watts, 'China's propaganda and disinformation landscape—2021 snapshot', *Selected Wisdom*, 19 November 2021, online.

39 The increasing involvement of private Chinese companies in foreign public-opinion warfare follows the commercialisation of the CCP's domestic information manipulation work. For the commercialisation of 'public opinion management', see Jessica Batke, Mareike Ohlberg, 'Message control', *ChinaFile*, 20 December 2020, online.

40 Nathaniel Gleicher, 'Meta's adversarial threat report', Meta, 1 December 2021, online. The Swiss Embassy in China denied that this person existed: Suranjana Tewari, 'Swiss embassy urges media to remove scientist fake news', *BBC*, 11 August 2021, online.

41 See further analysis by Doublethink Lab (online), which found that the company's intelligence service department (情报服务部) also provided intelligence mining, data analysis and foreign-language translations for the national security, public security and cyberspace ministries in the PRC.

42 James Pearson, Elizabeth Culliford, 'Facebook, Instagram remove Chinese network over fake "Swiss biologist" COVID claims', *Reuters*, 2 December 2021, online.

43 Gary King, Jennifer Pan, Margaret E Roberts, *How the Chinese Government fabricates social media posts for strategic distraction, not engaged argument*, Cambridge University Press, 27 July 2017, online.

44 As early as 2008, the Public Security Bureau in the city of Jiaozuo in Henan boasted of shifting public opinion to support the police after a negative post went up about a traffic offence fine; see Michael Bristow, 'China's internet spin doctors', *BBC News*, 16 December 2008, online. In 2020, the *New York Times* and *ProPublica* viewed leaked internal directives from the Hangzhou City Cyberspace Administration revealing that local Chinese governments activated online commentators to flood social-media websites to distract online conversations about Chinese Covid-19 whistleblower Dr Li Wenliang; see Raymond Zhong, Paul Mozur, Jeff Kao, Aaron Krolik, 'No "negative" news: how China censored the coronavirus', *New York Times*, 19 December 2020, online.

45 David Bandurski, 'Guidance of public opinion', *China Media Project*, 14 April 2020, online; Raphael Chan, 'Eliminating unformed threats', *China Media Project*, 16 September 2022, online.

46 See Albert Zhang's Twitter thread, online; Georgia Wells, Liza Lin, 'Pro-China Twitter accounts flood hashtag critical of Beijing Winter Olympics', *Wall Street Journal*, 8 February 2022, online.

47 Gleicher, 'Removing coordinated inauthentic behavior'. For analysis of this network, see Ben Nimmo, C Shawn Eib, Lea Ronzaud, 'Operation Naval Gazing', *Graphika*, 22 September 2020, online.

48 Gleicher, 'Removing coordinated inauthentic behavior'.

49 Beauchamp-Mustafaga, 'Cognitive domain operations: the PLA's new holistic concept for influence operations'; Adam Ni, Bates Gill, 'The People's Liberation Army Strategic Support Force: update 2019', *China Brief*, 29 May 2019, online; J Michael Cole, Shelley Shan, 'PRC steps up psychological warfare targeted at Taiwan', *Taipei Times*, 26 August 2011, online.

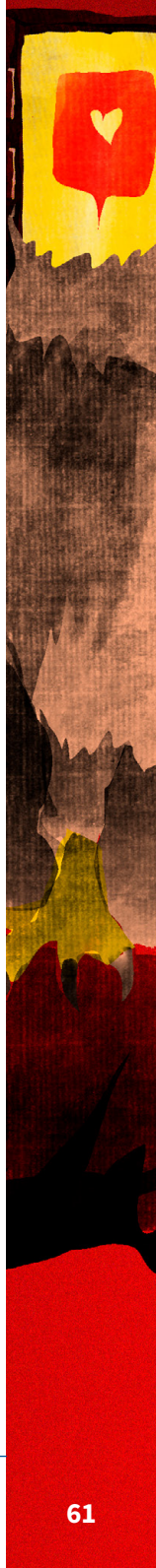
50 He Haixiang, 'The difficulties and paths of China's communication power construction in overseas social media (中国在海外社交媒体的传播力建设困境与路径)', *China Academic Journal Electronic Publishing House*, 2021, archived.

51 Wu Yifan, 'The Network Security Detachment of Shaoxing Public Security Bureau came to the School of Network Communication to discuss cooperation' (绍兴市公安局网安支队来网络传播学院洽谈合作), Zhejiang Yuexiu University, 24 March 2022, archived.

52 This article has since been deleted: 'The School of Network Communication held the eighth meeting of the first council of the Yuecheng District Internet Federation' (网络传播学院举行越城区网联会一届理事会第八次会议), Zhejiang Yuexiu University, 12 December 2019, archived.

53 'National Defense University' (中国人民解放军国防大学), *China Defence Universities Tracker*, ASPI, Canberra, online.

54 Sun Yixiang, Yu Yuanlai, 'Discussion on intelligent public opinion war' (刍议智能化舆论战), *China Military Network*, 31 March 2022, archived.



55 Taiwan Ministry of National Defense psychological warfare officier 'Ho' allegedly tracked down a number of Facebook pages and content farms made to look like Taiwanese ones but that were assessed to be operated by the CCP Central Propaganda Department: Paul Huang, 'Chinese cyber-operatives boosted Taiwan's insurgent candidate', *Foreign Policy*, 26 June 2019, online.

56 Marcel Schliebs, Hannah Bailey, Jonathan Bright, Philip N Howard, *China's public diplomacy operations: understanding engagement and inauthentic amplification of PRC diplomats on Facebook and Twitter*, University of Oxford, 11 May 2021, online.

57 We assess that the targeting of dissidents or voices critical of the CCP may be tasked to China's state security system. See reports on transnational repression: Zhang & Cave, 'Smart Asian women are the new targets of CCP global online repression'; Danielle Cave, Albert Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women', *The Strategist*, 6 November 2022, online. The US Department of Justice indicted MSS officers for transnational repression in March 2022. In one case, one MSS officer sought to interview Chinese dissidents in the US, which could have been used in CCP propaganda materials: 'Five individuals charged variously with stalking, harassing and spying on US residents on behalf of the PRC secret police', US Department of Justice, 16 March 2022, online.

58 Muyi Xiao, Paul Mozur, Gray Beltran, 'Buying influence: how China manipulates Facebook and Twitter', *New York Times*, 20 December 2021, online.

59 Ying-Yu Lin, an assistant professor at Taiwan's National Chung Cheng University, believed that a LinkedIn network promoting a pro-Beijing Taiwanese politician could be traced back to the PLASSF: Huang, 'Chinese cyber-operatives boosted Taiwan's insurgent candidate'.

60 In 2020, the *New York Times* and *ProPublica* viewed leaked internal directives from the Hangzhou City Cyberspace Administration revealing that local Chinese governments activated online commentators to flood social media websites to distract online conversations about Chinese Covid-19 whistleblower, Dr Li Wenliang: Zhong et al., 'No "negative" news: how China censored the coronavirus'.

61 Beauchamp-Mustafaga & Chase, *Borrowing a boat out to sea: the Chinese military's use of social media for influence operations*.

62 For example, OneSight worked with *China News Service*, which is a Chinese state media outlet supervised by the United Front Work Department: Jeff Kao & Mia Shuang Li, 'How China built a Twitter propaganda machine then let it loose on coronavirus'. Chinese state media also probably covertly contracted YouTube influencers to spread Covid-19 disinformation: Albert Zhang, 'China's cultural industry is being co-opted for disinformation operations', *The Strategist*, 8 February 2022, online.

63 'Fake cluster boosts Huawei', Graphika, 28 January 2021, online.

64 Ryan Fedasiuk, 'A different kind of army: the militarization of China's internet trolls', *China Brief*, 12 April 2021, online.

65 Spamouflage Twitter handles often used Twitter's default format, which usually combines the first name of the account with a random string of eight numbers. For examples, see archived.

66 For one example, see 'Vivian Morgan' Twitter profile, online.

67 It's unclear why this operation was named Operation Honey Badger (蜜獾行动) 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; see Mark Mazzetti, Adam Goldman, Michael S Schidt, Matt Apuzzo, 'Killing CIA informants, China crippled US spying operations', *New York Times*, 20 May 2017, online.

68 Beijing Qi An Pangu Laboratory Technology (北京奇安盘古实验室科技有限公司) is owned by Qi An Xin.

69 Cao Siqi, 'Evidence of US monitoring 45 countries, regions exposed by Chinese cybersecurity experts for the 1st time', *Global Times*, 23 February 2022, online.

70 Zhao Siwei, 'Evidence shows US' NSA behind attack on email system of leading Chinese aviation university', *Global Times*, 5 September 2022, online. For more information about Northwestern Polytechnical University, see ASPI's *China Defence University Tracker*, online.

71 Paul Szoldra, 'This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks', *Business Insider*, 16 September 2016, online.

72 Dan Goodin, 'NSA-leaking Shadow Brokers just dumped its most damaging release yet', *ArsTechnica*, 15 April 2017, online.

73 Matt Burgess, 'The mystery of China's sudden warnings about US hackers', *Wired*, 26 May 2022, online.

74 See NETRESEC's Twitter thread, online.

75 Zolan Kanno-Youngs, David E Sanger, 'US accuses China of hacking Microsoft', *New York Times*, 19 July 2021, online; John Hudson, Ellen Nakashima, 'US, allies accuse China of hacking Microsoft and condoning other cyberattacks', *Washington Post*, 19 July 2021, online.

76 Ministry of Foreign Affairs, 'MFA Coordinator for Cyber Affairs Wang Lei takes an exclusive interview with CCTV', PRC Government, 6 September 2022, online.

77 The account's earliest visible activity was in March 2021, and it has posted only anti-US propaganda disseminated by other accounts linked to pro-CCP networks.

78 For example, see 'Ada Rogers' Twitter profile (archived).

79 See this tweet on Twitter (archived). For background on the fake 'Milk Tea Alliance' report on Tumblr, see Albert Zhang's Twitter thread, online.

80 For example, see the profile photo of 'Branchff0845' (archived).

81 Targeting Guo Wengui has been a common characteristic of all Spamouflage-linked campaigns so far. For example, see the timeline history of 'Shannon Zimmerman' (archived).

82 TC Sottek, Janus Kopfstein, 'Everything you need to know about PRISM', *The Verge*, 17 July 2013, online.

83 See this tweet by a likely Spamouflage-affiliated Twitter account.

84 This narrative was posted on blogging websites before being shared on social media.

85 See these tweets.

86 Similar methods were used to disseminate pro-Chinese police articles to flood reporting of the Safeguard Defenders report on CCP transnational repression. See Albert Zhang's Twitter thread and this archived tweet.

87 Zhang Yanping, 'America's hegemony disease—a door for eavesdropping that never stops' (美国霸权病——永不关闭的监听之门), *Huanqui*, 3 June 2021 online.

88 Cave & Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women'.

89 See, for example, 'DFSGDFHFD', *Twitter*, online; see link between #GenocideGames and Spamouflage on Albert Zhang's Twitter thread, online.

90 Naomi Nix, Jeremy B Merrill, Joseph Menn, 'MAGA porn, hate for Trump: China-based accounts stoke division', *Washington Post*, 1 November 2022, online.

91 ASPI analysis of the APAC 3 dataset disclosed in October 2022 to the Twitter Moderation Research Consortium.

92 See Li Bijian's Twitter post, archived.

93 Stanford Internet Observatory and Graphika initially analysed the pro-Western datasets disclosed by Meta and Twitter and suspected it was run by the US military: *Unheard voice: evaluating five years of pro-Western covert influence operations*, Graphika, 24 August 2022, online. Those datasets were later attributed by Meta to the US military: 'Quarterly adversarial threat report', Meta, November 2022, online.

94 Fergus Ryan, Ariel Bogle, Albert Zhang, Jacob Wallis, *#StopXinjiang Rumors: the CCP's decentralised disinformation campaign*, ASPI, Canberra, 2 December 2021, online.

95 Uren et al., *Tweeting through the Great Firewall*.

96 Wallis et al., *Retweeting through the Great Firewall*.

97 Xi Jinping told Chinese propaganda officials in an August 2013 speech that 'judging from the Prism and XKeyscore, the energy and scale shown by the US's internet operation far exceeded people's imagination'. See Jun Mai, 'How Xi Jinping looks to the Communist Party to plug cybersecurity gaps', *South China Morning Post,* 13 August 2021, online.

98 Devin Thorne, '1 key for 1 lock: the Chinese Communist Party's strategy for targeted propaganda', *Recorded Future*, 28 September 2022, online.

99 Hu Zhengrong, Tian Xiao, 'The construction of China's international communication discourse system in the new era of hierarchical classification and grouping' (分层分类分群 新时代中国国际传播话语体系的构建), *Prof. Hu Zhengrong's Blog*, 10 September 2021, archived.

100 'Chinese state-sponsored cyber espionage activity supports expansion of regional power and influence in Southeast Asia', *Insikt Group*, 8 December 2021, online; Matt Burgess, 'China is relentlessly hacking its neighbors', *Wired*, 28 February 2023, online.

101 ASPI first identified this behaviour: Zhang & Cave, 'Smart Asian women are the new targets of CCP global online repression'; Cave & Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women'. ASPI's attribution was then supported by former Twitter staff: Adam Rawnsley, 'Why is Twitter shutting down Chinese activists' accounts?', *Rolling Stone*, 9 December 2022, online.

102 'Beijing 996 business hours' refers to business hours between 9 am and 9 pm, Monday to Saturday: Lin Qiqing, 'Long hours lead to labor disputes for China's startups', *Sixth Tone*, 23 August 2017, online.

103 Coco Feng, 'Chinese social media to display user locations based on IP address, including platforms from ByteDance and Zhihu', *South China Morning Post*, 17 April 2022, online.

104 Joy Dong, 'China's internet censors try a new trick: revealing users' locations', *New York Times*, 18 May 2022, online.

105 Zhang, 'The CCP's information campaign targeting rare earths and Australian company Lynas'.

106 See archived screenshot.

107 Social listening services offered by Meltwater.

108 Zhihu account, online, archived.

109 Zhihu post, online.

110 Yancheng Police Detachment's official Toutiao account, online.

111 See a report published by the Xinfeng County People's Government about responses to police-related online public opinion, online.

112 See Washington Post reporting.

113 Meng Hongwei (孟宏伟), a former Vice Minister of Public Security, was the President of Interpol at that time. Uren et al., *Tweeting through the Great Firewall*.

114 Uren et al., *Tweeting through the Great Firewall*.

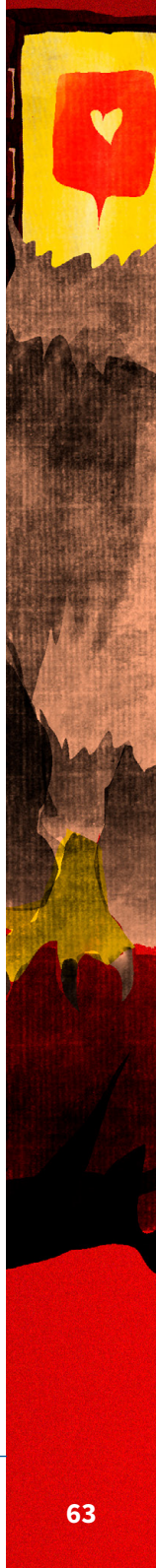
115 See tweet posted by 'DFSGDFHFD', an account we assessed to be very likely affiliated with Chinese influence operations.

116 'National public security news propaganda seminar held in Yancheng, Jiangsu' (全国公安新闻宣传研修班在江苏盐城举行), *The Paper*, 5 June 2018, archived.

117 'National public security news propaganda seminar held in Yancheng, Jiangsu'.

118 'Central Politics and Law Commission notification! Shantou Politics and Law won the honour of Advanced in the new media work of politics and law!' (中央政法委通报！汕头政法获政法新媒体工作'先进'荣誉！), *Shantou Politics and Law*, 24 October 2020, archived.

119 'China's political and legal system runs the cyber army "fifty cents" [which] is expected to be incorporated and integrated' (中国政法系统办网军'五毛'有望收编整合), *Voice of America*, 6 September 2018, online. In 2019, Chen Yixin suggested that China's political and



legal system strengthen its 'cyber army' to safeguard online ideology: Chen Yixin, *Fight the tough battle to prevent and defuse political security risks* (打好防范化解政治安全风险攻坚战), Chang Anjian Central Political and Legal Commission, 10 April 2019, online.

120 King et al., *How the Chinese Government fabricates social media posts for strategic distraction, not engaged argument*.

121 The term 'spin doctors' was first used by the *BBC*: Michael Bristow, 'China's internet spin doctors', *BBC News*, 16 December 2008, online.

122 The Cyberspace Administration of China has a history of managing internet commentators to manipulate online conversations on Chinese social media. See Raymond Zhong, Paul Mozur, Jeff Kao, Aaron Krolik, 'No negative news: how China censored the coronavirus', *New York Times*, 19 December 2020, online.

123 'Yancheng Cyberspace Adminstration Service Unit social benefit evaluation and website editor-in-chief debriefing meeting held' (盐城市互联网信息服务单位社会效益评价暨网站总编辑述职会召开), *Sohu*, 31 January 202, archived.

124 'Yancheng City Party Committee Cyberspace Administration held the 2020 annual democratic life meeting' (盐城市委网信办召开2020年度民主生活会), *Sohu*, 7 February 2021, archived.

125 'The 5th National Network Public Opinion Summit Forum: The Cyberspace Administration of the Yancheng Municipal Party Committee won the Excellent Award for Network Public Opinion Guidance for the first time' (第五届全国网络舆情高峰论坛 : 盐城市委网信办首获网络舆论引导优秀奖), *JSTV*, 22 June 2019, archived.

126 'The 5th National Network Public Opinion Summit Forum: The Cyberspace Administration of the Yancheng Municipal Party Committee won the Excellent Award for Network Public Opinion Guidance for the first time' (第五届全国网络舆情高峰论坛 : 盐城市委网信办首获网络舆论引导优秀奖).

127 Yui Aragaki previously bookmarked a Zhihu post warning men not to take their girlfriends travelling unless their relationship is strong enough or they'll break up. He bookmarked another Zhihu post about 'common sense' facts about women that men might not know.

128 At least before 8 January 2022, the date of the first self-taught higher education examinations.

129 The tweet is archived.

130 For examples, see: 'Report on the work of curbing the spread of the epidemic and maintaining the results of prevention and control' (遏制疫情扩散蔓延守住防控成果工作情况汇报), online; 'Report on the work of poverty alleviation in XX County in 20XX' (XX县20XX年脱贫攻坚工作情况汇报), online; 'Report on the work of trade unions in XX Province' (XX省工会工作情况汇报), online.

131 Article 18 of 'Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management' (互联网信息内容管理行政执法程序规定), Cyberspace Administration of China, 29 July 2021, archived.

132 Eliot Chen, 'Microsoft's long past and uncertain future in China', *The Wire China*, 7 November 2021, online. The MPS requests are listed on *GitHub*, online.

133 'YCCG-2012-CS228-01 Yancheng Public Security Bureau public opinion special push service announcement' (YCCG-2012-CS228-01盐城市公安局舆情专项推送服务中标公告), *BidCenter*, 8 January 2021, archived.

134 'Beijing Wisdom Starlight Information Technology Co., Ltd.' (北京智慧星光信息技术有限公司), *D.T.Lake Equity Investment*, undated, archived; 'Beijing Wisdom Starlight Information Technology Co., Ltd.' (北京智慧星光信息技术有限公司), *Guomai E-Government Network*, undated, archived.

135 Nimmo, 'Removing coordinated inauthentic behavior from China and Russia'.

136 'Twitter accounts of European politicians hijacked to spread CCP propaganda', Institute of Strategic Dialogue, 22 April 2022, online.

137 China Aerospace Studies, 'China establishes military–civilian integrated innovation center for cyberspace security', Department of the Air Force, US Government, 23 January 2018, online.

138 'Zhai Wenjing, co-founder of Dataview, was elected as a member of the Big Data Operation and Maintenance (Cybersecurity) Committee of the All-China Federation of Industry and Commerce' (数据观联合创始人翟文静入选全国工商联大数据运维 (网络安全) 委员会委员), *Shangyexinzhi*, 17 June 2020, archived.

139 'Zhai Wenjing, co-founder of Dataview, was elected as a member of the Big Data Operation and Maintenance (Cybersecurity) Committee of the All-China Federation of Industry and Commerce' (数据观联合创始人翟文静入选全国工商联大数据运维 (网络安全) 委员会委员).

140 Department of Defense, 'DOD releases list of additional companies, in accordance with Section 1237 of FY99 NDAA', US Government, 28 August 2020, online.

141 Liang Chen, 'Cybersecurity concept stock Qi An Xin was officially listed on the Science and Technology Innovation Board, and the opening rose by more than 115%' (网安概念股奇安信正式挂牌科创板 开盘涨幅逾115%), *Beijing News*, 22 July 2020, online.

142 'Yancheng Public Security and 360 Enterprise Security Group signed a strategic cooperation agreement' (盐城公安与360企业安全集团签署战略合作协议), Yancheng Municipal Public Security Bureau, 21 January 2019, archived.

143 'Yancheng Public Security and 360 Enterprise Security Group signed a strategic cooperation agreement' (盐城公安与360企业安全集团签署战略合作协议), Yancheng Municipal Public Security Bureau, 21 January 2019, archived.

144 'Zhou Hongyi's "Unreconciled": It took four months to rebuild 360 Enterprise Security Group' (周鸿祎的'不甘心' : 用四个月重建360企业安全集团), *Tencent Cloud*, 5 September 2019, online.

145 'Qi An Xin' (奇安信), Jiangsu Government Procurement Network, 17 December 2020, archived.

146 'Yancheng Public Security and 360 Enterprise Security Group signed a strategic cooperation agreement' (盐城公安与360企业安全集团签署战略合作协议).

147 In 2017, China Communications Information Center, Tongji University, Beijing Qi Anxin Technology Co. Ltd (360) and *China Communications News* established the Transportation Big Data System and Security Laboratory. This laboratory used the National Engineering Laboratory of Big Data Collaborative Security Technology as a platform to carry out research and development and application promotion of transportation infrastructure and vehicle intelligent security, blockchain security authentication technology, public-opinion monitoring and internet information content security; archived.

148 'Big Data Collaborative Security Technology National Engineering Laboratory Technical Committee meeting successfully held' (大数据协同安全技术国家工程实验室技术委员会会议成功举行), *NERCBDS*, 4 January 2021, archived. The National Defense University is designated very high risk for its work training PLA personnel, according to ASPI's *China Defence Universities Tracker*, online.

149 'Qi Xiangdong was appointed as the director of the National Engineering Laboratory for Big Data Security' (齐向东出任大数据安全国家工程实验室主任), *Xinhuanet*, 26 May 2017, archived.

150 See Appendix 4 on Qi An Xin's links to the Chinese Government.

151 *Qi An Xin Technology Group Co. Ltd 2021 annual report* (奇安信科技集团股份有限公司2021 年年度报告), Shanghai Stock Exchange, 2022, online.

152 David Bandurski, 'Guidance of public opinion', *China Media Project*, 14 April 2020, online.

153 'Inner Mongolia Association for Science and Technology launches network security and public opinion security training' (内蒙古科协开展网络安全和舆情安全培训), China Association for Science and Technology, 17 August 2020, archived.

154 Nathaniel Gleicher, 'Meta's adversarial threat report', Meta, 1 December 2021, online.

155 'There is no national security without cybersecurity! Silence helps the 2019 National Cyber Security Publicity Week' (没有网络安全就没有国家安全！无声信息助力2019年国家网络安全宣传周), Sichuan Silence Information Technology, 4 November 2019, archived.

156 See this blog post that we assessed to be very likely part of Spamouflage.

157 See these tweets.

158 See this tweet.

159 Elise Thomas, Albert Zhang, Jacob Wallis, *Automating influence on Covid-19*, ASPI, Canberra, 24 August 2020, online.

160 'The Bvp47—a top-tier backdoor of US NSA Equation Group', *Pangu Lab*, 23 February 2022, online.

161 Didi Kirsten Tatlow, 'Digital paper in China covers contentious issues, now in English', *New York Times*, 5 April 2016, online.

162 'The US stealing scandal strikes again! It has ravaged the world's internet for nearly 20 years and was exposed by Chinese researchers' (美窃密丑闻又起！肆虐世界网络近20年，被中国研究员曝光), *Sohu*, 26 February 2022, online.

163 See archived profile page.

164 Baidu Images appears to have scrapped the image from the Zhongguancun Blue Navy Civilian Integration Industry Promotion Association website.

165 The company aims to become the world's number 1 cybersecurity company, according to its 2021 annual report: *Qi An Xin Technology Group Co. Ltd 2021 annual report* (奇安信科技集团股份有限公司2021 年年度报告).

166 See page 56 for examples of Qi An Xin's international clients.

167 Jiang Jie, 'China's cybersecurity companies eye Belt and Road opportunities', *People's Daily Online*, 26 August 2019, online.

168 'Received the Outstanding Contribution Award for two consecutive years! Qi An Pangu receives appreciation from Huawei' (连续两年获得突出贡献奖！奇安盘古获华为致谢), *Aqniu*, 25 October 2021, archived.

169 'Qi An Xin and HUAWEI CLOUD launched a mobile security office solution for government and enterprises' (奇安信联合华为云推出政企移动安全办公解决方案), *Qi An Xin*, 25 September 2020, archived.

170 'Invisible champion cultivation path under the construction of new development pattern' (新发展格局构建下的隐形冠军培育路径), National Development and Reform Commission, 29 November 2021, online. For analysis of China's hidden champions, see Alexander Brown, *China relies on 'little giants' and foreign partners to plug stubborn technology gaps*, MERICS, 24 February 2022, online.

171 Huawei terminal security partners, in Chinese, archived.

172 Huawei terminal security partners, in English, archived.

173 'Direct attack on the "Belt and Road": Qi An Xin reached a cooperation with Indonesian AG Group' (直击"一带一路"：奇安信与印尼AG集团达成合作), Qi An Xin, 24 April 2019, archived.

174 William C Rempel, Alan C Miller, 'FBI details Democratic fund-raising abuses', *Los Angeles Times*, 6 February 2000, online.

175 'Janet Reno's stewardship of the Justice Department: a failure to service the ends of justice', House Government Reform Committee, US Congress, 13 December 2000, online.

176 The connection between Liu Chaoying and Major General Ji Shengde is mentioned in 'Janet Reno's stewardship of the Justice Department: a failure to service the ends of justice'. For details about the PLA's political warfare operations, see Mark Stokes, Russell Hsiao, 'The People's Liberation Army General Political Department: political warfare with Chinese characteristics', *Project 2049*, 14 October 2013, online.

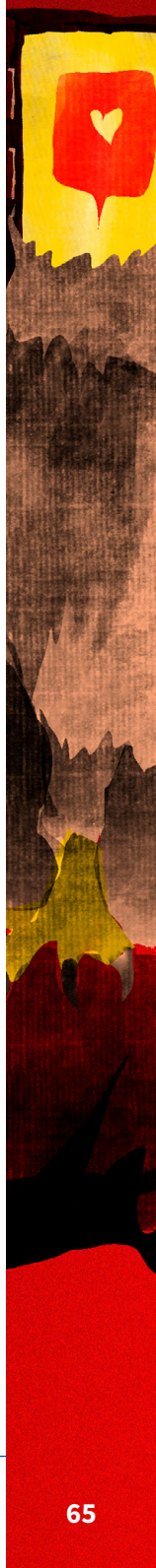
177 'Direct attack on the "Belt and Road": Qi An Xin reached a cooperation with Indonesian AG Group' (直击"一带一路"：奇安信与印尼AG集团达成合作).

178 According to the *Sydney Morning Herald*, Tomy Winata amassed a fortune through businesses operated on behalf of the Indonesian military: Lindsay Murdoch, Tom Hyland, 'Dili tycoon deal triggers alarm', *Sydney Morning Herald*, 3 May 2009, online. In February 2023, Huang Zhenyao (黄珍耀), the head of the Putian Municipal United Front Work Department, met with Tomy Winata, among others, as part of an economics and trade delegation: 'Fu Chaoyang, secretary of the Putian Municipal Party Committee, led an economic and trade delegation to visit locals in Indonesia and held an economic and trade meeting to discuss projects', United Front Work Department of Putian Municipal Party Committee, 16 February 2023, archived.

179 The full list of countries wasn't disclosed, but representatives from the United Arab Emirates, Tunisia, Egypt, Kuwait, Morocco and Zambia were identified: 'Defense military attachés from eighteen countries visit QI-ANXIN Group', Qi An Xin, 30 March 2022, archived.

180 The full list of countries wasn't disclosed, but representatives from the United Arab Emirates, Tunisia, Egypt, Kuwait, Morocco and Zambia were identified: 'Defense military attachés from eighteen countries visit QI-ANXIN Group', Qi An Xin, 30 March 2022, archived.

181 'Qi Anxin's international business won a large order of 70 million' (奇安信国际业务拿下七千万大单), *Sina News*, 31 December 2021, online.



182 'Qi Xiangdong: Self-reliance in network security technology is an inevitable choice to effectively resolve international trade disputes' (齐向东：网络安全科技自立是有效解决国际贸易纷争的必然选择), *iFeng*, 25 December 2021, online.

183 'Qi Anxin: A subsidiary company won the bid for the construction project of a cybersecurity command center in a capital city of an overseas country' (奇安信：下属公司中标海外某国家首都城市网络安全指挥中心建设项目), *Sina News*, 9 November 2022, online.

184 'Defense military attachés from eighteen countries visit QI-ANXIN Group'.

185 Gao Jiachen, 'Wu Yunkun, President of Qi Anxin Group: The surge in digital demand will detonate the development of the global network security market' (奇安信集团总裁吴云坤：数字化需求激增将引爆全球网络安全市场发展), *China Securities Journal*, 9 November 2022, online; Jiang Ji, 'China's cybersecurity companies eye Belt and Road opportunities', *People's Daily Online*, 26 August 2019, online.

186 'Qi Xiangdong talks about military–civilian integration: gathering multiple forces to create a new model' (齐向东谈军民融合：凝聚多元力量打造新模式), *China Army Work Online*, 16 April 2018, archived.

187 'Cyberspace Administration of China and Indonesia's National Network and Cryptography Agency signed a memorandum of cooperation in the field of network security' (中国国家互联网信息办公室与印尼国家网络与密码局签署网络安全领域合作备忘录), Cyberspace Administration of China, 15 January 2021, archived.

188 'Cyberspace Administration of China and Thailand's National Cyber Security Office sign a memorandum of understanding on cyber security cooperation' (中国国家互联网信息办公室与泰国国家网络安全办公室签署网络安全合作谅解备忘录), Cyberspace Administration of China, 5 July 2022, online.

189 See Appendix 3: Possible Spamouflage linkages to APT41.

190 Michael Brissenden, 'Australia spied on Indonesian President Susilo Bambang Yudhoyono, leaked Edward Snowden documents reveal', *ABC News*, 18 November 2013, online; James Risen, Laura Poitras, 'Spying by NSA ally entangled US law firm', *New York Times*, 15 February 2014, online; 'Indonesia leader says Australia spying damaged ties', *BBC News*, 19 November 2013, online; Kanupriya Kapoor, 'Australia's gone too far spying on shrimp trade talks, Indonesia says', *Reuters*, 17 February 2014, online.

191 深入把握总体国家安全观 (In-depth grasp of the overall national security concept), 22 November 2021, archived.

192 Beauchamp-Mustafaga & Chase, *Borrowing a boat out to sea: the Chinese military's use of social media for influence operations*.

193 Joshua Kurlantzick, 'China wants your attention, please', *Foreign Policy*, 5 December 2022, online.

194 He Haixiang, the Dean of the School of Network Communication at Zhejiang Yuexiu University of Foreign Languages, has suggested that the CCP should support the expansion of Chinese social media platforms abroad to increase the CCP's discourse power: He Haixiang, 'The difficulties and paths of China's communication power construction in overseas social media'. Meta has previously warned of threat actors seeking to capitalise on the public's fear of information operations to create false perceptions of widespread manipulations on US-based platforms: 'Threat report: the state of influence operations 2017–2020', Meta, May 2021, online.

195 For example, see these tweets posted by inauthentic accounts very likely affiliated with Spamouflage.

196 Johan Burger, 'TikTok gaining ground as a marketing platform in Africa', Nanyang Technological University, 25 October 2021, online.

197 Laura Silver, Kat Devlin, Christine Huang, *Unfavorable views of China reach historic highs in many countries*, Pew Research Center, 6 October 2020, online; Natasha Kassam, *Lowy Institute Poll 2022*, Lowy institute, Sydney, 29 June 2022, online.

198 Zhang, 'Pro-CCP inauthentic social media accounts shift focus to the Quad'.

199 Zhang, 'The CCP's information campaign targeting rare earths and Australian company Lynas'.

200 He Haixiang, *The difficulties and paths of China's communication power construction in overseas social media* (中国在海外社交媒体的传播力建设困境与路径).

201 'Hangzhou Waixuan overseas social media account operation and maintenance public bidding documents' (杭州外宣海外社交媒体账号运维公开招标文件), September 2021, archived.

202 See the timeline of the Hangzhoufeel Twitter account, online.

203 Hangzhofeel Twitter account, online.

204 Casey Newton, 'What Instagram really learned from hiding like counts', *The Verge*, 27 May 2021, online.

205 Stefan Heumann, 'Why Social Media Platforms Should Be Treated as Critical Infrastructures', *Medium*, 13 October 2018, online; The information ecosystem broadly comprises the individuals, organisations and their relationships that contribute to the communication of information in a society. That includes influencers, TV broadcasters, news media organisations, websites and social-media platforms. See Thomas H Davenport, 'Information ecology', *Internet Archive*, 1997, archived.

206 'Disinformation Code', *DIGI*, online.

207 'Security of Critical Infrastructure Act 2018', *Federal Register of Legislation*, online.

208 'Telecommunications (Interception and Access) Act 1979', Australasian Legal Information Institute, online. For ASPI's analysis of exceptional access laws, see Tom Uren, *The future of assistance to law enforcement in an end-to-end encrypted world*, ASPI, Canberra, 23 February 2022, online.

209 'Australia-US CLOUD Act Agreement', *Australian Government Department of Home Affairs*, online.

210 Lesley Seebeck, Emily Williams, Jacob Wallis, *Countering the Hydra: a proposal for an Indo-Pacific hybrid threat centre*, ASPI, Canberra, 7 June 2022, online.

211 As an example, see China's cyber ranges: Dakota Cary, *Downrange: a survey of China's cyber ranges*, Center for Security and Emerging Technologies, September 2022, online.

212 Schliebs et al., *China's public diplomacy operations: understanding engagement and inauthentic amplification of PRC diplomats on Facebook and Twitter.*

213 Hamilton 2.0 Dashboard, Alliance for Securing Democracy at the German Marshall Fund of the United States, online.

214 'What are Canarytokens', *Canarytokens*, 23 October 2021, online.

215 Joshua Beaman, 'Log4j hunting & indicators', Security Blue Team, December 2021, online.

216 Rufus Brown, Van Ta, Douglas Bienstock, Geoff Ackerman, John Wolfram, *Does this look infected? A summary of APT41 targeting US state governments*, Mandiant, 8 March 2022, online; Danny Palmer, 'Within hours of the Log4j flaw being revealed, these hackers were using it', *ZDNet*, 8 March 2022, online.

217 Sarah Fitzpatrick, Kit Ramgopal, 'Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says', *NBC News*, 5 December 2022, online.

218 See this tweet, for example, from an account very likely to be affiliated with Spamouflage.

219 See this *Medium* article posted by an account very likely to be affiliated with Spamouflage.

220 Carly Page, 'China-backed APT41 compromised "at least" six US state governments', *TechCrunch*, 9 March 2022, online.

221 See this forum post, archived.

222 See this tweet, for example.

223 See this tweet posted by Intrusion Truth's Twitter account.

224 Cave & Zhang, 'Musk's Twitter takeover comes as the CCP steps up its targeting of smart Asian women'.

225 'TeamT5 Information Operation White Paper III: China's social manipulation outside the Great Firewall', *TeamT5*, 15 October 2020, online.

226 Ye Zhanqi, Zhao Runhua, 'Spat grows between internet security-firm bigwigs', *Caixin Global*, 22 August 2019, online.

227 'Qi An Xin Technology Group Co. Ltd 2021 annual report' (奇安信科技集团股份有限公司2021 年年度报告).

228 'Qi An Xin Technology Group Co. Ltd 2021 annual report' (奇安信科技集团股份有限公司2021 年年度报告).

229 'Qi An Xin', Ai Qi Cha, archived.

230 'National Military & Civil Integration Industrial Investment Fund', Ai Qi Cha, online.

231 'China Electronics Corporation', *China Defence Universities Tracker*, ASPI, Canberra, online.

232 Department of the Treasury, 'Issuance of Executive Order addressing the threat from securities investments that finance certain companies of the People's Republic of China & related FAQs; Introduction of Non-SDN Chinese Military-Industrial Complex Companies List', US Government, 3 June 2021, online.

233 'Qi An Xin', Ai Qi Cha, archived.

234 'Beijing Xicheng District branch of the State-owned Assets Supervision and Administration Commission', Ai Qi Cha, archived.

235 'Qi An Xin', Ai Qi Cha, archived.

236 'Hexie Chengzhang is the National Council for Social Security Fund of the PRC', Ai Qi Cha, online.

237 'About Qi An Xin' (关于奇安信), Qi An Xin, no date, archived.

238 'Qi An Xin reached a strategic cooperation with the third research institute of the Ministry of Public Security' (奇安信与公安部三所达成战略合作), *Jiemian*, 19 October 2020, archived.

239 'Build a safe and reliable public security information communication network' (打造安全可靠的公安信息通信網), *Qi An Xin*, archived.

240 Adam Cozy, *China's cyber capabilities: warfare, espionage, and implications for the United States*, US–China Economic and Security Review Commission, 17 February 2022, online.

241 'Registration examination and safety training services' (註冊考試與安全培訓服務), Qi An Xin, archived.

242 'Under the policy of China Information Security Evaluation Center, the field of CISP-PTE offence and defence is full of energy' (CISP-PTE攻防领域在中国信息安全测评中心政策下，劲头十足), *Sahoo*, 30 April 2019, archived.

243 'Member information', Zhongguancun Science and Technology Innovation Smart Military Industry Technology Innovation Strategic Alliance (ZASDI), archived; 'About us', ZASDI, archived.

244 'Technical expert—JW Agency' (技术专家-JW机关), *Zhaopin*, 31 March 2022, online.

245 'Qi Xiangdong talks about military–civilian integration: gathering multiple forces to create a new model' (齐向东谈军民融合：凝聚多元力量打造新模式)'; 'To help the construction of national defense in cyberspace, the three strategic centers of 360 settled in Mianyang' (助力網絡空間國防建設，360三大戰略中心落戶綿陽), *China Military Network*, 29 March 2018, archived.

246 'Qi An Xin', Ai Qi Cha, archived.

247 *Qi An Xin 2021 annual report*.

248 *Qi An Xin 2021 annual report*.

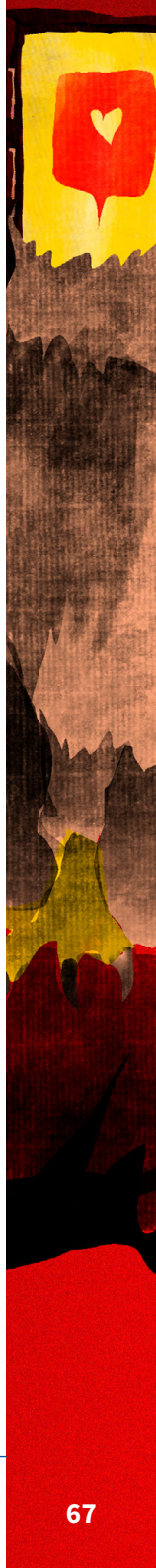
249 'The list of members of the new CPPCC National Committee was announced Qi An Xin Chairman Qi Xiangdong was selected' (新一届全国政协委员名单公布 奇安信董事长齐向东入选), *NetEase*, 18 January 2023, archived.

250 The CPPCC is the CCP's peak united front forum for supervision over non-CCP parties, mass organisations and prominent personalities: Alex Joske, *The party speaks for you*, ASPI, Canberra, 9 June 2020, online.

251 The All-China Federation of Industry and Commerce is subordinate to the CCP's United Front Work Department (UFWD): '习近平：关于《中共中央关于党的百年奋斗重大成就和历史经验的决议》的说明 决议全文' [Jinping: The full text of the resolution on the 'Resolution of the Central Committee of the Communist Party of China Concerning the Major Achievements and Historical Experience of the Party's Centennial Struggle'], CPP Central Committee, online.

252 'Zhai Wenjing, co-founder of Dataview, was elected as a member of the Big Data Operation and Maintenance (Network Security) Committee of the All-China Federation of Industry and Commerce' (数据观联合创始人翟文静入选全国工商联大数据运维 (网络安全) 委员会委员), *Shang Ye Xin Zhi*, 17 June 2020, archived.

253 *Qi An Xin 2021 annual report*.



254 The China Confidentiality Association is supervised by the National Administration of State Secret Protection of the PRC, which is also the CCP Central Committee's Office of Secrets Protection Committee. '中共中央保密委员会办公室): 中国保密协会简介' [Introduction to the China Confidentiality Association, 1 January 2020, online; 'Announcement of the "Notice of the State Council on the Establishment of Institutions"' (《国务院关于机构设置的通知》公布), *People's Daily*, 25 March 2018, archived.

255 The Cyber Security Association of China is supervised by the CAC: Cyber Security Association of China, '中国网络空间安全协会章程' [Constitution of China Cyberspace Security Association], online; 'Association leaders', CSAC, 5 December 2019, archived.

256 'Leader of Internet Society of China', Internet Society of China, 9 September 2021, online; the Internet Society of China is supervised by the Ministry of Industry and Information Technology (工业和信息化部), according to its charter, online.

257 'Qi Xiangdong was appointed as the director of the National Engineering Laboratory for Big Data Security' (齐向东出任大数据安全国家工程实验室主任), *Xinhuanet*, 26 May 2017, archived.

258 'Wu Yunkun, President of Qi Anxin Technology Group' (奇安信科技集团总裁吴云坤), Nanjing University of Aeronautics and Astronautics, 13 April 2021, archived.

259 Ouyang Shijia, 'Qihoo 360 expanding cloud security business', *China Daily*, 30 January 2018, online.

260 'Wu Yunkun, President of Qi Anxin Technology Group' (奇安信科技集团总裁吴云坤).

261 'Wu Yunkun, President of Qi Anxin Technology Group' (奇安信科技集团总裁吴云坤).

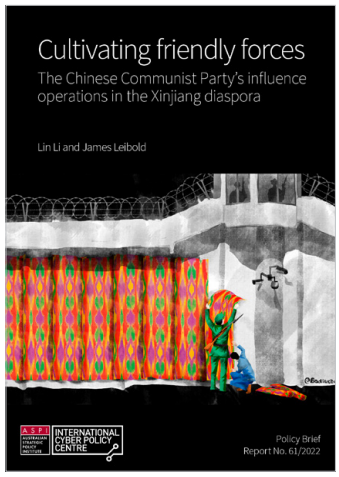
262 The People's Public Security University of China is subordinate to the Ministry of Public Security: 'History', People's Public Security University of China, no date, online.

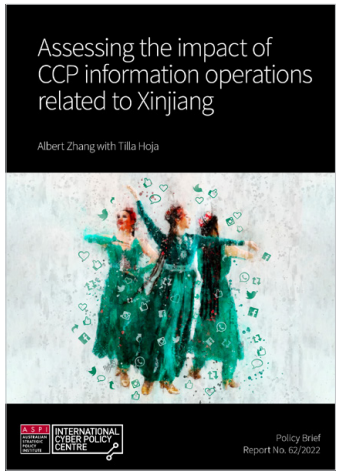
263 'World Information Security Conference' (世界信息安全大会), *INSec World*, no date, archived.

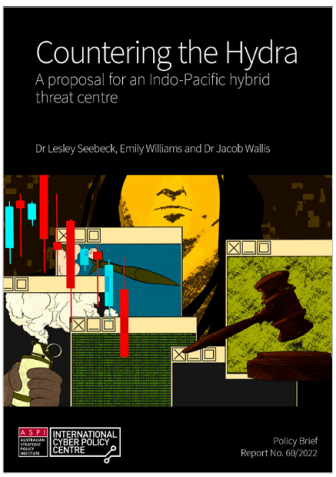
Acronyms and abbreviations

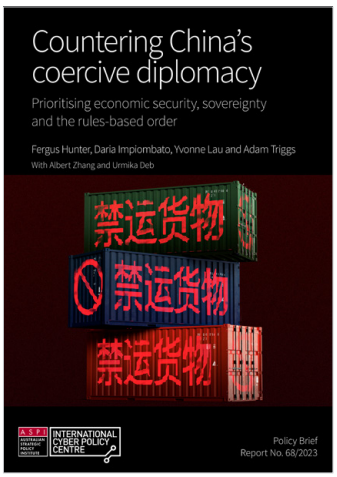
AI	artificial intelligence
APEC	Asia–Pacific Economic Cooperation
APT	advanced persistent threat
BRI	Belt and Road Initiative
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
CEC	China Electronics Corporation
CIA	Central Intelligence Agency
CNITSEC	China Information Technology Security Evaluation Centre
CPPCC	Chinese People's Political Consultative Conference
EU	European Union
MFA	Ministry of Foreign Affairs
MPS	Ministry of Public Security
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PLA	People's Liberation Army
PLASSF	People's Liberation Army Strategic Support Force
PRC	People's Republic of China

Some previous ICPC publications









ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE