中国简报 China Brief
a journal of analysis and information
The JAMESTOWN FOUNDATION

VOLUME 19 • ISSUE 16 • SEPTEMBER 6, 2019

IN THIS ISSUE:



## Chinese Covert Social Media Propaganda and Disinformation Related to Hong Kong

*By John Dotson*

### Introduction: "Coordinated Inauthentic Behavior" Related to the Protest Movement in Hong Kong

On August 19, the microblogging platform Twitter announced the suspension of 936 accounts originating in the People's Republic of China (PRC), which the company identified as part of an "information operation focused on the situation in Hong Kong." The company stated that these accounts "were deliberately and specifically attempting to sow political discord in Hong Kong, including undermining the legitimacy and political positions of the protest movement on the ground," and further asserted that "we have reliable evidence to support that this is a coordinated state-backed operation" (Twitter Blog, August 19).

On the same day, Facebook announced that—acting on information provided by Twitter—it had taken down fifteen accounts, pages, or groups "involved in coordinated inauthentic behavior as part of a small network

that originated in China and focused on Hong Kong." The company further asserted that the organizers "behind this campaign engaged in a number of deceptive tactics… to manage Pages posing as news organizations, post in Groups, disseminate their content, and also drive people to off-platform news sites… Although the people behind this activity attempted to conceal their identities, our investigation found links to individuals associated with the Chinese government" (Facebook Newsroom, August 19).


*Image: A screen shot from one of the accounts disabled by Twitter. This account, for the fictitious media organization "Dream News," editorializes that the protestors who broke into and vandalized Hong Kong's Legislative Council building on July 1 were acting on behalf of unspecified "forces [that] hide behind the scenes." (Source: Twitter)*

These announcements were followed three days later by a statement from Google, the parent company of Youtube, that it had taken down 210 channels on the video posting site "as part of our ongoing efforts to combat coordinated influence operations." The company stated that this action was taken "when we discovered [that] channels in this network behaved in a coordinated manner while uploading videos related to the ongoing protests in Hong Kong [which was] consistent with recent observations and actions related to China announced by Facebook and Twitter" (Google Blog, August 22).

The exposure of this coordinated covert operation has shed further light on how the social media realm has emerged as one of the newest fronts for PRC state-directed propaganda and disinformation efforts intended to bolster the interests of the ruling Chinese Communist Party (CCP). **[1]** It also reveals much about the narratives surrounding the Hong Kong protest movement that the CCP wishes to promote to both domestic and foreign audiences. As such, the themes and methods of this social media campaign merit closer examination.

**PRC Covert Propaganda and Disinformation Through Social Media**

The covert social media campaign employed by PRC entities against the Hong Kong protest movement is not the first of its kind: the Russian government's use of social media disinformation to manipulate opinion and sow divisions in other countries has been well-established. **[2]** Furthermore, PRC actors have themselves sought to covertly use both traditional and social media to influence public opinion in places such as Taiwan (Straits Times, April 2; Taiwan Sentinel, April 8). However, the accounts suspended in August are noteworthy for attempting to direct disinformation towards a broader international audience.

*Propaganda and Disinformation Themes*

Material drawn from the suspect social media accounts avoids substantive discussion of issues motivating the Hong Kong protest movement (the draft extradition law, universal suffrage, etc.), relying instead on emotive language and imagery intended to stimulate patriotic feelings, fear, or disgust. Five propaganda themes stand out prominently in the PRC covert social media campaign surrounding events in Hong Kong:

1. All Chinese persons, whether within or beyond the borders of the PRC, stand in unified support of Chinese government policies towards Hong Kong.
2. The protest movement is secretly controlled by the United States—which seeks to bring about a "color revolution" (颜色革命, *yanse geming*) intended to overthrow the Hong Kong city administration, to separate Hong Kong from the rest of China, and to weaken China as a whole.
3. The protestors are terrorists, equipped by the United States, who employ brutal violence and potentially lethal weapons against both police officers and the general public in Hong Kong.
4. The Hong Kong police are courageous heroes protecting the public from violence and anarchy.
5. The protestors are identified with various types of verminous insects.

The first four points are all consistent with PRC overt propaganda. However, in official propaganda outlets the second and third points are generally made with oblique hints rather than explicit statements. For example, an August 12 commentary in the flagship CCP newspaper *People's Daily* asserted that foreign "black hands" had "attempted to interfere in China's internal affairs by stirring up trouble, creating chaos and instigating riots in Hong Kong…[t]hey have used people in Hong Kong as 'chess pieces' and 'cannon fodder' for their political schemes… [t]hey instigated extreme radicals to make trouble, trained them, provided them with weapons, and made false speeches to ignite hostile emotions among the people" (People's Daily, August 12). The "black hands" are not specifically named, but it is clearly implied that they belong to the United States.

The fifth point listed above—the dehumanization of protestors as insects—is not a feature of official PRC propaganda. However, this is a consistent theme in covert social media material, as well as in overtly hosted (if not explicitly endorsed) material, in which protestors are repeatedly labeled as "cockroaches" (甲由, *yuezha*) or "locusts" (蝗虫, *huangchong* or 蚂蚱, *mazha*) *(see accompanying images)*. Such an

identification is intended to provoke disgust—and potentially, to carry the implication that such vermin deserve extermination.


*Images above: Screen shots from accounts taken down by Facebook, on grounds that they were suspected of being part of an orchestrated PRC-directed propaganda and misinformation campaign directed against the Hong Kong protest movement. Left: Some violent actions (subway attacks, the shooting of a woman in the eye) carried out by Hong Kong police or pro-administration triad gangs are ascribed to protestors; and the protestors themselves are dehumanized as "cockroaches" causing "chaos."*
*Right: Protestors are compared to terrorists, with a caption that reads: "Although the weapons are different, the results are the same!" (Source: Facebook Newsroom)*

*Language and Platform Selection, and Their Potential Significance*

Many of the suspect accounts featured content in English, as well as in Chinese script *(see accompanying images).* The reasons for this are unclear, but it may indicate either that the content was intended to shape opinion abroad, and/or that it was directed towards bilingual target audiences in Hong Kong and overseas diaspora communities. Some of the suspect English-language accounts and content were presented as if coming from sources from outside China (CBS San Francisco, August 20)—and therefore may have been intended to support a narrative of widespread international outrage against the protestors.

The use of these particular platforms is also noteworthy: Western-operated social media sites like Twitter and Facebook are restricted within the PRC (although not in Hong Kong), and sites and apps such as Weibo and WeChat are far more commonly used by Chinese consumers. Therefore, the covert social media campaign was likely intended primarily to target opinion overseas, rather than at home. However, if the campaign was

directed to an international audience, the outlandish propaganda themes and the crude nature of the English-language content (poor grammar, etc.) likely limited its overall effectiveness.

*Use of Virtual Private Networks by Campaign Participants*

Ironically, one of the deceptive methods associated with the social media disinformation campaign was the use of virtual private networks (VPNs), a common tool employed to disguise the internet protocol (IP) address associated with particular web searches and postings. Although they are still used within the PRC, VPNs are officially banned, and their usage can result in fines, lowered "social credit" scores, and potential arrest. However, their usage was a hallmark of the suspect accounts targeted in August: as announced by Google, "We found use of VPNs and other methods to disguise the origin of these accounts and other activity commonly associated with coordinated influence operations" (Google Blog, August 22). Twitter stated that "many of these accounts accessed Twitter using VPNs [and some] accounts accessed Twitter from specific unblocked IP addresses originating in mainland China" (Twitter Blog, August 19).


*Images above: English-language Twitter accounts from PRC state-controlled newspapers, presenting disinformation and propaganda regarding the Hong Kong protests. Left: An August 11th post from* China Daily, *alleging that the protester in the left foreground is firing a U.S.-manufactured grenade launcher. Such falsified content is intended to support PRC state media narratives that Hong Kong protesters are violent terrorists, and that the United States is fueling the unrest from behind the scenes. (Source: China Daily Twitter Page) Right: An August 16th post from* People's Daily, *providing a link to a multi-lingual (English and Mandarin) rap music video. The nationalistic lyrics reiterate CCP propaganda themes regarding Hong Kong: that the unrest is part of a U.S.-directed "color revolution" intended to spread chaos and separate the territory from China, and that protestors are treasonous "locusts." (Source: People's Daily Twitter Page)*

**PRC Overt Propaganda Channeled Through Twitter**

The account and channel suspensions announced in August by Twitter, Facebook, and Google do not affect the overt use of these platforms by PRC state entities. Through their overt accounts, PRC media outlets may continue to spread propaganda and disinformation about the Hong Kong protest movement: either through direct news coverage, or by hosting content from nominally independent third parties. *(For two recent examples of such Twitter content by PRC state-controlled newspapers, see the images immediately above.)*

However, while these PRC state entities will still be free to post news content through their accounts, their use of future social media advertising may be at least partially curtailed. On the same day that it announced the account suspensions, Twitter further announced that it would cease accepting advertising from "state-controlled news media entities"—defined as entities subject to state editorial control, but omitting publicly-funded outlets with independent editorial control, such as Voice of America or Deutsche Welle (Twitter Blog, August 19).

**Conclusion**

The actions taken by Twitter, Facebook, and Google in August revealed an unusual display of solidarity and coordinated action on the part of three of the world's biggest social media and internet content companies. The action taken by these U.S.-based social media companies cuts against an ethos of unregulated speech that these companies have invoked in the past—and more importantly, impacts their corporate profits. These companies are likely reacting, at least in part, to negative press attention relating to earlier interactions with the Chinese government: both Facebook and Twitter have been stung this year by criticisms for hosting advertisements and promoting propaganda tweets from Chinese state sources (Next Web, August 19). Twitter was further criticized in June for suspending Chinese-language accounts critical of the PRC government in advance of the 30th anniversary of the Tiananmen Square Massacre (Business Insider, June 2).

The account suspensions announced by these U.S. internet media companies have drawn a predictably harsh response from PRC officials. On August 20, PRC Foreign Ministry spokesman Geng Shuang (耿爽) asserted that "Chinese media use overseas social media to elaborate on China's policy [and] tell China's story," and that PRC media outlets expressed "the attitude of the 1.4 billion Chinese on the situation in Hong Kong" (PRC Foreign Ministry, August 20). In a statement on August 28, Liu Liehong (刘烈宏), Director of the CCP Central Cyberspace Affairs Commission Office, issued a richly ironic statement that described the suspensions as an attack on China's freedom of speech rights (Xin Jing Bao, August 28).

Although this particular PRC covert social media disinformation network has been at least partially disrupted, it is very unlikely that this is the end of the story. The low cost / low risk nature of such operations makes them an attractive option for authoritarian governments interested in swaying or polarizing opinion in more

open societies—or at least, for sowing confusion and attendant inaction on the part of persons who might otherwise adopt positions contrary to CCP interests. Future days are likely to see further "coordinated inauthentic behavior" from cyber actors doing the bidding of the CCP.

*John Dotson is the editor of* China Brief*. Contact him at: cbeditor@jamestown.org.*

**Notes**

**[1]** For purposes of this article, the terms "covert operation" and "covert" are defined per official terms employed by the U.S. Government: "covert operation—an operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor." [See: U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms* (updated July 2019), pp. 54. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.] The term "disinformation" is defined per the terms of *Merriam-Webster's Dictionary*: "false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth." [See: *Merriam-Webster.com*, entry for "disinformation." https://www.merriam-webster.com/dictionary/disinformation.] For a broader discussion of these issues, see: Dean Jackson, "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News'," National Endowment for Democracy, October 17, 2017. https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

**[2]** Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* ("Mueller Report"), Vol. 1 Section 2 ("Russian 'Active Measures' Social Media Campaign"), pp. 14-35 (March 2019). https://www.justice.gov/storage/report.pdf.

***

## Taiwan Public Opinion Polling Regarding Forced Unification with China

*By Timothy Rich and Andi Dahmer*

### Introduction: China's Historic Stance on Unification with Taiwan

The position taken by the government of the People's Republic of China (PRC) regarding Taiwan's status is clear, and enshrined in the preamble of the country's constitution: "Taiwan is part of the sacred territory of the People's Republic of China. It is the inviolable duty of all Chinese people, including our compatriots in Taiwan, to accomplish the great task of reunifying the motherland." **[1]** Although PRC officials have never given a public timeline for this unification, they have consistently reiterated their commitment to a "One Country, Two Systems" (一国两制, *Yi Guo Liang Zhi*) framework—one that Taiwan officials, including current President Tsai Ing-wen (蔡英文), have repeatedly rejected (Nikkei Asian Review, January 5).

This could change in the future: China's political and economic rise, coupled with the removal of term limits for Chinese Communist Party (CCP) General Secretary Xi Jinping, potentially changes the strategic calculus for prolonging the status quo. Xi stated in 2013 that a solution cannot wait forever, and reiterated in early 2019 that the PRC reserved all options to achieve unification (China Brief, February 15). The PRC has continued to prepare for a military solution to the Taiwan situation, and earlier this year Xi ordered the People's Liberation Army (PLA) to be ready for such military action (NPR, January 2; Straits Times, January 6).

With these matters in mind, we asked polling recipients in Taiwan about their concerns regarding the possibility of forced unification: a situation in which Chinese threats or coercive actions give Taiwan leaders no choice but to concede to permanent PRC sovereignty over Taiwan. Asking about one's preferred status for Taiwan constitutes one of the core questions asked on most public opinion surveys in Taiwan since democratization. In recent years, around 15 percent of the population (at most) has stated support for unification, even after a prolonged status quo (Taiwan News, January 3). However, detailed public opinion research on forced unification remains rare. Our own research reveals significant concern about forced unification among Taiwan's population, albeit with stark differences along the partisan divide of Taiwan politics.


*Image: In a demonstration held in the southern Taiwan city of Kaohsiung in April 2019, participants carry signs rejecting the "One Country, Two Systems" framework promoted by Beijing. (Source: RFA)*

**The Prospect of Forced Unification**

Considerable debate exists regarding the likelihood of PRC action to compel reunification with Taiwan. In 2018, author Deng Yuwen stated that China could act to seize Taiwan by 2020, a year prior to the 100th anniversary of the founding of the CCP (South China Morning Post, January 3, 2018). This year, Peter Gries and Tao Wang suggested that the situation is so tenuous that wishful thinking alone could provoke war

(Foreign Affairs, February 15). Most analysts assume that Beijing would only pursue forced unification if it were convinced that inaction would lead to a *de facto* permanently independent Taiwan. Denny Roy, Michael Beckley, J. Michael Cole, and Ian Easton, among others, question whether China could or would want to take Taiwan by force; while Tanner Greer argues that a key component for the success of any invasion—the element of surprise—would be impossible to achieve due to the narrow time windows offered by weather conditions in the Taiwan Strait. **[2]**

However, several factors could alter such calculations. For example, domestic challenges in the PRC could lead officials to deflect attention by appealing to Chinese nationalism over the issue of Taiwan. Military advancements may also convince Chinese leaders that a swift victory is possible before the United States could come to Taiwan's aid; or that the PLA has developed the capabilities to deter, if not defeat, U.S. forces in the region. Xi's desire to cement his legacy with unification on his watch could also motivate such actions. Furthermore, actions outside of China also could influence a push for forced unification—and even if PRC officials currently accept an indefinite status quo in private, unexpected actions by the United States or Taiwan could change their perspective.

The Trump administration has strengthened informal ties with Taiwan, and recently advanced a series of large arms sales to the island (China Brief, July 31; DSCA, August 20). Likewise, increased U.S. Congressional support signals a stronger commitment from the United States towards Taiwan, as demonstrated by: the National Defense Authorization Act (2018) authorizing senior-to-senior military engagement and training between U.S. and Taiwan forces; support for military transfers and sales to Taiwan; and the Taiwan Travel Act (2018) supporting increased contacts with Taiwan government officials (Taiwan Sentinel, July 27, 2018). These closer ties have drawn a harsh response from PRC officials: for example, in early 2018 Li Kexin, a minister at the PRC Embassy in Washington, stated that a U.S. Navy vessel docked in a Taiwanese port would be grounds for war (South China Morning Post, January 3, 2018). Such steps, and possible continued and strengthened security commitments offered by the United States to Taiwan, could convince PRC leaders that they must act while any hope of unification remains.

Actions taken by Taiwan officials also could lead to a PRC response, especially if Chinese officials are worried about growing Taiwanese national identity. A recent survey showed that three-quarters of respondents in Taiwan view Taiwan and China as separate countries (South China Morning Post, June 21, 2017). Currently, the Tsai Administration's efforts to maintain the country's international space and *de facto* independence—including the continued refusal to accept Chinese demands for adherence to the so-called "92 Consensus"—may not be enough for the PRC to take action. However, a Tsai bolstered by perceived American security guarantees—and appealing to her party's base in the 2020 presidential campaign—could lead the PRC to view force as its last remaining option for unification, framing such intervention as a defensive war to protect Chinese sovereignty.

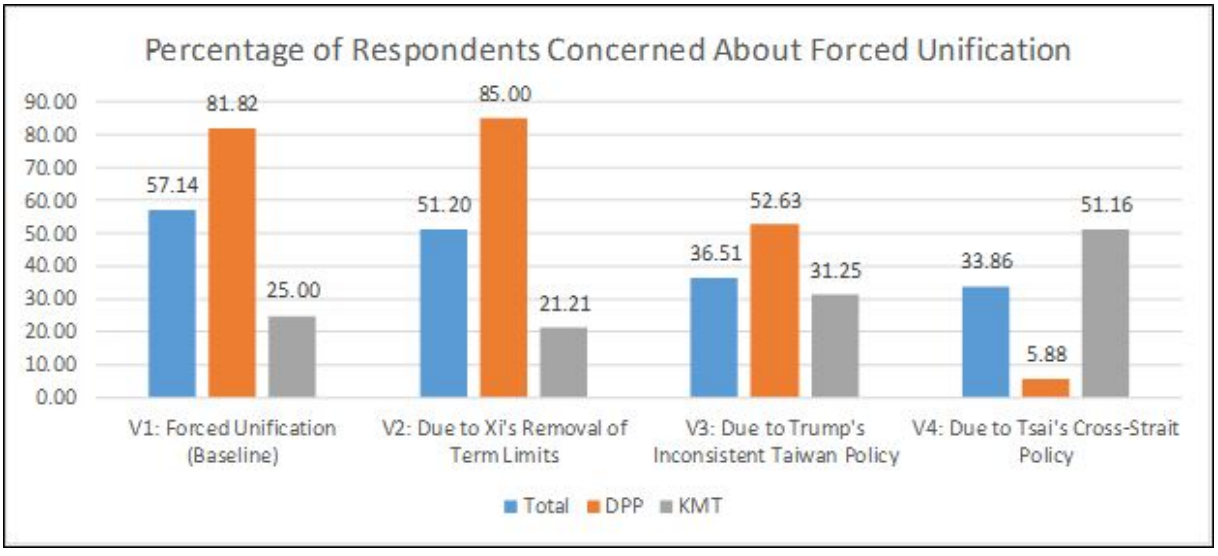
**Concerns About Forced Unification Among Taiwan Citizens**

We wanted to survey concerns in Taiwan about forced unification, under three possible scenarios. The first scenario dealt with perceptions as to whether Xi Jinping, no longer bound to term limits, might feel emboldened to take actions leading to forced unification. The second scenario asked respondents whether they thought that shifts in Trump Administration policy might lead the United States to abandon its commitments to Taiwan. Finally, the third scenario considered whether or not Tsai Ing-wen's cross-strait policy would provoke PRC actions.

To gauge concerns regarding the prospect of forced unification, we surveyed 504 Taiwan residents in April via an experimental web survey conducted by PollcracyLab. Respondents received one of four randomized prompts and were asked to evaluate their feelings about the given prompt on a five-point Likert scale (strongly disagree to strongly agree). The four prompts were as follows:

- Version 1 (V1): "I am concerned about forced unification with the People's Republic of China."
- Version 2 (V2): "Due to the removal of term limits on Xi Jinping's rule, I am concerned about forced unification with the People's Republic of China."
- Version 3 (V3): "Due to Donald Trump's inconsistent Taiwan policy, I am concerned about forced unification with the People's Republic of China."
- Version 4 (V4): "Due to Tsai Ing-wen's cross-strait policy, I am concerned about forced unification with the People's Republic of China."

The figure below presents the percentage of total respondents that agreed or strongly agreed with each version *(in blue)*. It also differentiates between responses from self-identified supporters of the historically independence-leaning Democratic Progressive Party (DPP) *(in orange)* and the historically unification-leaning Kuomintang (KMT) *(in gray)*.



Among respondents as a whole, we see a slim majority (57.14 percent) state that they are concerned about forced unification, with the three conditional prompts (V2, V3, and V4) eliciting less concern from the general population. As might be expected, we see higher levels of concern about forced unification among DPP supporters than KMT supporters, with a difference of over threefold between responses from the two parties in the baseline scenario.

Among supporters of the DPP (the party historically favoring independence), rates of concern dropped when forced unification was framed as the result of Trump's policies, although a narrow majority of DDP supporters (52.63 percent) still held this concern. Very few DPP supporters were concerned about the prospect of unification as a result of Tsai's policies. By contrast, among supporters of the KMT (the party historically supporting unification), concerns about forced unification as a result of Tsai's policies were more than double the baseline response. It is reasonable to expect that partisan identification would drive evaluations under the V4 scenario, regardless of Tsai's cross-strait policy. However, the divergent rates of concern between DPP and KMT supporters in both the baseline (V1) scenario and the removal of term limits for Xi scenario (V2) also show significant gaps along partisan lines.

It is important to note that our survey was conducted prior to the mass protests in Hong Kong that broke out in June 2019, in response to a proposed new extradition law and other grievances (China Brief, June 26). We were not able to capture how these subsequent actions influenced the concerns of Taiwan residents regarding forced unification; however, we would expect that many Taiwan citizens would view the developments in Hong Kong as a sign of what could happen under unification with the PRC.

**Conclusion**

Overall, our results suggest that there is significant public concern in Taiwan over the prospect of forced unification. However, that concern is heavily conditioned by both partisan leanings and by perceptions of how key political leaders (Xi, Trump, and Tsai) may potentially influence the context of unification. The results also suggest that it may be difficult for the Tsai Administration to respond to such concerns, as Taiwan's government has little control over the perceptions and interests, or future decision-making, of outside leaders such as Xi and Trump. Additionally, factional and generational divisions within the DPP further complicate efforts to identify what scenario might instigate actions towards forced unification.

*Timothy S. Rich is an Associate Professor of Political Science at Western Kentucky University. His research focuses on the domestic and international politics of East Asia, with an emphasis on Taiwan and South Korea. He has published over 50 peer-reviewed articles and is a frequent contributor to policy and academic outlets in the United States, Taiwan, United Kingdom, and Australia.*

*Andi Dahmer, a 2018 Harry S. Truman Scholar, recently graduated from Western Kentucky University. Her primary research focuses on the diplomatic recognition of Taiwan as it relates to Central America, with broader research interests in Taiwan and the Koreas.*

**Notes:**

**[1]** National People's Congress of the PRC, "Preamble," Constitution of the People's Republic of China [*Zhonghua Renmin Gongheguo Xianfa*], 1982, last amended 2018.

**[2]** See: Denny Roy, 'Prospects for Taiwan Maintaining its Autonomy under Chinese Pressure,' *Asian Survey*, Vol. 57 No. 6, University of California, Berkeley Institute of East Asian Studies, November/December 2017, pp. 1135-1158; Michael Beckley, 'The Emerging Military Balance in East Asia: How China's Neighbors Can Check Chinese Naval Expansion,' *International Security*, Vol. 41, No. 2, Massachusetts Institute of Technology, pp. 78-119; J. Michael Cole, 'What Happens if China Tried to Invade Taiwan,' The National Interest, April 10, 2019, https://nationalinterest.org/blog/buzz/what-happens-if-china-tried-invade-taiwan-51852; Ian Easton, *The China Invasion Threat: Taiwan's Defense and American Strategy in Asia*, 2nd ed., Eastbridge Books, April 2019; Tanner Greer, 'Taiwan Can Win a War with China,' September 25, 2018, Foreign Policy, https://foreignpolicy.com/2018/09/25/taiwan-can-win-a-war-with-china/.

***

## "Key Individuals Management" and the Roots of China's Anti-Muslim Surveillance System

*By Emile Dirks*

### Introduction

The repression of Xinjiang's Uighur population by the government of the People's Republic of China (PRC) continues to horrify world opinion. Along with interning an estimated one million people in a network of re-education camps, the Chinese state has built extensive systems of daily surveillance directed at the region's Muslims (China Brief, March 14, 2017; China Brief, November 5, 2018). **[1]** Police inspections of local homes, blacklists of suspect Muslims, and biometric data collection are widespread.

Previous research has illustrated how such policies have their roots in earlier (and ongoing) repression campaigns against Falun Gong and other religious groups (China Brief, February 1). However, evidence now suggests that these systems of social surveillance and repression also originated in programs directed at wider groups of Chinese citizens, identified as "key individuals" (重点人员, *zhongdian renyuan*). Systems of "key population management" (重点人口管理, *zhongdian renkou guanli*) possess many of the features associated with Xinjiang's security state: profiling, extensive personal and biometric data collection, and location-based tracking.

Drawing on dozens of local government notices, government bid tenders and promotional material from Chinese technology companies, a composite picture of key population management can be assembled. By examining key individuals management, we can learn more about the roots of the PRC's anti-Muslim surveillance programs—programs that one day may be directed against ever-increasing new segments of the Chinese public.

**Who Are "Key Individuals"?**

Although "key individuals" are a topic of frequent discussion in mainland Chinese academic literature, the concept has been little discussed outside China. **[2]** The term therefore requires some explanation. According to the 2007 *Key Population Management Guidelines* (公安部重点人口管理规定, *Gongan Bu Zhongdian Renkou Guanli Guiding*) issued by the PRC Ministry of Public Security (hereafter "Guidelines"), key individuals are persons suspected of threatening national security or social stability (Junan County Government, October 18, 2017). Article 3 of the *Guidelines* associates 20 kinds of people into two broadly defined general categories: potential national security threats and serious criminal offenders. Article 4 specifies three other groupings as key individuals: individuals involved in disputes with the potential for dangerous escalation; people released from prison or re-education through labor camps; and users of illegal drugs.

While the *Guidelines* establish the general parameters of whom key individuals are, local government notices indicate which groups are routinely placed under surveillance. Examining more than 70 online notices from 26 of China's 34 administrative regions published between 2011 and 2019 reveals the following most frequently mentioned key individual groups: **[3]**

| | English | Chinese |
|---|---|---|
| Criminal & Administrative Law Offenders | • People on parole<br>• People in community corrections<br>• Users of illegal drugs | • 刑满释放人员<br>• 社区矫正人员<br>• 吸毒人员 |
| Political Groups | • Citizen petitioners<br>• "Stability maintenance" involved people<br>• "Terror" involved people | • 信访人员<br>• 涉稳人员<br>• 涉恐人员 |
| Other | • Members of "evil cults" (ex. Falun Gong)<br>• "Floating populations" (domestic migrants)<br>• Unstable mentally ill individuals | • 邪教人员<br>• 流动人员<br>• 肇事肇祸精神人员 |

*Image: Categories of Key Individuals Mentioned in Local Government Notices. (Source: Author's Notes.)*

From these notices, we can see that local authorities interpret key individuals categories broadly: for example, domestic migrants, citizen petitioners, and the mentally ill are not specifically mentioned in the *Guidelines*, but they are frequently discussed in local government notices.

**Data Collection and Databases in Key Individuals Management**

Regardless of which groups are targeted, data collection lies at the heart of key individuals management. Government notices routinely instruct local officials and public security officers to work in concert to collect information on key individuals, a process referred to as "investigating" (排查, *paicha*) or "assessing and investigating" (摸底排查, *modi paicha*) (Tianjin Baodi Government, December 12, 2018). As data collection efforts have grown, so too has the need for specialized police-run key individuals databases.

A core feature of the PRC's campaign against Uighurs has been the creation of vast police databases of information on Uighur citizens (Human Rights Watch, May 1). Disturbing as these databases are, their origins predate the current anti-Muslim campaigns and extend back to the mid-2000s, with the introduction of machine-readable national ID cards (Keesing Journal of Documents & Identity, 2010). These so-called "second generation" ID cards (第二代身份证, *di er dai shenfenzheng*) allowed personal data to be stored electronically and shared among government offices, including the Public Security Bureau. It was then that the Chinese government first began collaborating with domestic tech firms to create digital databases of key individuals—including religious minorities.

One of the first nation-wide key individuals databases was the "Drug User Online Dynamic Control Alert System" (吸毒人员网上动态管控预警系统, *Xidu Renyuan Wangshang Dongtai Guankong Yujing Xitong*) (PRC Ministry of Public Security, August 29, 2006). Launched in 2006 as part of China's "People's War on Drugs" (人民禁毒战争, *Renmin Jindu Zhanzheng*), the Dynamic Control System (DCS) contains personal information on more than two million registered users of illegal drugs, including those held in or released from extrajudicial drug detention centers. Government reports, media coverage and academic scholarship give a sense of what data are collected in the DCS: basic personal information, residential address, and history of drug use and participation in drug treatment programs. **[4]**

The DCS is also one of the earliest examples of ID-based location tracking and biometric data collection aimed at key individuals—predating the collection of DNA samples from Uighurs by a decade. Whenever a registered user of drugs uses their national ID number to conduct a computer-based transaction (such as checking in to a hotel room), the nearest public security offices are alerted. Police officers can then identify the person's location, intercept them, and conduct a urine drug test, the results of which can be added to the person's file (International Drug Policy Consortium, February 2017).

*Image: Profiles of persons in Zhengzhou City (Henan Province) flagged for warning alerts. (Source: China Security and Protection Industry Association, Fall 2017)*

Biometric data collection is not limited to urine drug test results. Article 6 of the 2008 "Drug User Registration Methods" (吸毒人员登记办法, *Xidu Renyuan Dengji Banfa*) refers to collecting fingerprints and DNA data on individuals whose identities police cannot verify (*Legal Daily*, September 24, 2009). As early as November 2017, reports from Hainan indicated that police had begun collecting DNA samples from registered drug users as part of regular key individuals management operations (*Hainan Daily*, November 25, 2007).

**Chinese Tech Firms as Contractors for the PRC's Domestic Surveillance System**

The DCS quickly became a template for other key individuals databases—and Chinese tech firms have become extensively engaged as contractors working to support these government programs. Absent a purchased copy, direct examination of this software is impossible. One exception is Hongda (宏达) Software's "Public Security Personnel Information Management Work System" (公安人员信息管理工作系统, *Gongan Renyuan Xinxi Guanli Gongzuo Xitong*), released in 2008. **[5]** The software's user help document—complete with extensive screenshots of the system's interface—is freely available for download and provides a clear insight into how the software allows police to monitor a range of key individuals, including former prisoners, users of drugs, and foreigners.

One of the key individuals categories listed in Hongda's system are "practitioners of evil cults" (邪教人员, *xiejiao renyuan*). The PRC government launched a campaign of imprisonment, intimidation, and torture against members of the Falun Gong spiritual movement in 1999, and the Hongda example illustrates that by 2008 (a period when surveilling Falun Gong adherents was a priority for local public security organs in the lead up to the Beijing Olympics) the Chinese government was already working with domestic tech companies

to monitor religious minorities. To this end, the Management Work System permitted police to catalogue known practitioners according to precise criteria: who introduced them to the movement; where and with whom they practiced; and their "level of [spiritual] obsession" (痴迷程度, *chimi chengdu*). Such rankings now read as disturbing precursors to the police assessments of Uighurs as "safe", "average", and "unsafe" (The Guardian, April 11).

Since the release of Hongda's Information Management System, police interest in key individuals databases has only grown. Key word searches on China Bidding (中国采购与招标网, *Zhongguo Caigou yu Zhaobiao Wang*) and Bid Center (采招网, *Cai Zhao Wang*) turned up twenty two public tenders for key individuals databases or related surveillance products, issued by local government offices in 15 different provinces or centrally administered cities between October 2015 and June 2019. **[6]**

China's tech companies have responded to these business opportunities. In addition to Hongda Management Software, a cursory online search revealed five other firms offering key individuals-related software for public security organs:

- Shenzhen Yuanzhongrui Technology (深圳源中瑞科技)
- Beijing Sensingtech LLC (北京深醒科技有限公司)
- Zhejiang Yidiantong Information Technology Ltd. (浙江亿点通信息科技有限公司)
- CASIC Guangda Technology Ltd. (北京航天光达科技有限公司)
- Shenzhen Harzone Technology Ltd. (深圳市华尊科技有限公司)

The website for Yidiantong Information Technology's "Key Individuals Control" (重点人员管控, *Zhongdian Renyuan Guankong*) (KIC) provides the most detailed overview of one of these systems (Zhejiang Yidiantong 'Product Page,' undated). **[7]** Like other key individuals databases, KIC can record extensive personal information on registered persons, including social media accounts and bank account details. And like the DCS, KIC is integrated with the information systems of hotels, internet cafes, airports, and railway stations to enable both real-time data sharing and targeted police actions against registered individuals.

Yidiantong's website also indicates that the range of key individuals groups has continued to expand:

| English | Chinese |
|---|---|
| • Terror- or Xinjiang-involved people<br>• National security targets<br>• Extremists<br>• Mentally ill people involved in stirring up trouble<br>• Petitioners<br>• High risk migrants<br>• Foreigners<br>• Users of drugs<br>• Online targets<br>• People released from jail<br>• Members of "evil cults" (ex. Falun Gong<br>• Others | • 涉恐涉疆<br>• 国保重点<br>• 极端人员<br>• 肇事肇祸精神病<br>• 信访人员<br>• 高危流口<br>• 境外人员<br>• 吸毒人员<br>• 网上重点<br>• 刑事解教<br>• 邪教人员<br>• 其他人员 |

*Image: Key Categories of People Mentioned in Yidiantong's Key Individuals Control System (Source: Zhejiang Yidiantong 'Product Page,' undated)*

That people from Xinjiang, petitioners, migrants, the mentally ill, foreigners, and online targets do not appear in the 2007 *Guidelines* suggests that tech companies are building databases in response to extralegal demands from public security agencies, rather than public policy documents or statutory law.

As the market for key individuals databases increases, so too has the range of related products, including China's often-discussed facial recognition cameras. However, as this research suggests, it is police officers and low-level bureaucrats—armed with computers, clipboards, and handheld data entry devices—who continue to be the most reliable eyes of the PRC's growing state apparatus for methodically enumerating China's most marginalized members of society. For this reason, one of the most unsettling aspects of Yidiantong's Key Individuals Control system is its related "Community Alert" (社区警务, *Shequ Jingwu*) program. **[8]** By using Community Alert, police can create simple two-dimensional maps of apartment complexes, and associate particular key individuals—whether petitioners, foreigners, users of drugs, "cult" members, or the mentally ill—with specific apartment units. Such maps further facilitate the forms of intrusive surveillance, unannounced interrogations, and biometric data collection detailed in local government notices.

**Conclusion**

Key individuals management and data collection did not begin in Xinjiang, nor is it likely to end there. Software programs first deployed against users of drugs in the mid-2000s were soon directed against members of Falun Gong. By the late 2010s, the net had widened to ensnare the Uighurs of Xinjiang. Now these tools of data collection and surveillance, refined in Kashgar and Urumqi, are being redeployed across

the rest of China. It is unclear what key individuals these systems will target next. What is clear is that in the absence of robust media or judicial oversight—or any other institutional checks on the Communist Party's domestic security apparatus—key individuals management will continue to metastasize, bringing ever greater swaths of the Chinese public under its control.

*Emile Dirks is an independent researcher based in Toronto, Canada whose work focuses on extrajudicial detention and government surveillance in the People's Republic of China.*

**Notes**

**[1]** Although estimates vary widely in regards to the number of Uighur citizens detained by the PRC government, United Nations representatives have cited the figure of one million as a best estimate, based on reports from international human rights organizations (BBC, August 10; Amnesty International, September 2018).

**[2]** For illustrative examples, see: Shen Huizhang, "On Police Cooperation in the Dynamic Management of Floating Populations," (论流动人口动态管理的警务协作) *Journal of Political Science and Law* vol. 27, issue 5, 2010 pp. 101-5; Chen Jian and Hu Changhai, "Analysis on Countermeasures for Dynamic Control of Key Individuals Under New Circumstances," (浅析新形势下重点人员动态管控对策), Henan Police Academy Journal vol. 22, issue 4, 2013, pp.57-60; Guo Yujing, "Thoughts on Strengthening and Innovating Key Individuals Management Work," Shandong Police Academy Journal, vol. 2, issue 122, 2012, pp.138-143; Pu Yanmei and Li Changliang, "Analysis of Current Issues in Key Individuals Management" (当前重点人口管理存在问题原因分析), Yunnan Police Academy Journal, vol. 2, issue 79, 2010, pp.75-8; Wang Zhanjun, "Research on the Construction of Key Individuals Dynamic Control Service Systems," Journal of the Criminal Investigation Police University of China, vol. 2, issue 142, 2018, pp. 55-60.

**[3]** On request, the author can provide interested researchers with examples of these government notices, with corresponding links.

**[4]** For illustrative examples, see: Guangdong Drugs Administration, "Methods for Controlling Users of Illegal Drugs," June 26, 2019, http://www.gd.gov.cn/zwgk/zcfgk/content/post_2524013.html; China National Anti-Drug Foundation, "Lushan Anhui Anti-Drug Brigade Strengthens Dynamic Controls System" (安徽：砀山禁毒大队加强动态管控 严防漏管失控), January 4, 2017, http://www.nncc626.com/2017-01/04/c_129431988.htm; Lu Yang, "Concern Over Chinese Drug Abusers' Rights and Interests," VOA China, September 30, 2011, https://www.voachinese.com/a/article-20110930-aizhixing-report-130858758/788438.html; Sun Guan, "Composition of the Dynamic Control Systems for Users of Illegal Drugs," (吸毒人员动态管控机制的构成), Journal of the Jiangsu Police Academy, vol. 22, issue 2, pp. 27-31.

**[5]** See product page for Hongda Software Information Management System, accessed September 6, 2019, http://www.inmis.com/product_view.asp?id=1283.

**[6]** The China Bidding URL is http://www.chinabidding.org.cn. Bid Center can be accessed at https://bidcenter.com.cn. On request, the author can provide interested researchers with examples of these bid tenders, with corresponding links.

**[7]** Zhejiang Yidiantong, 'Key Individuals Control Product Page,' undated, accessed September 6, 2019, http://www.zjyidt.com/Product/Product.
**[8]** Ibid.

***

## Looking Beyond Commodities Exports: China Increases Its Engagement with Brazil

*By Shanti Salas*

### Introduction

In June 2019, the People's Republic of China (PRC) scored a victory in its relationship with Brazil when it gained the latter country's support for the PRC's candidate to lead the United Nations Food and Agriculture Organization (FAO), over candidates put forward by France and Georgia (Brazil Ministry of Agriculture, June 23, 2019). The PRC's candidate, Qu Dongyu, won 108 votes (over France's runner-up candidate with 71 votes) to become the next director-general of the FAO. The significance of Brazil's support for the PRC over France in the international body is especially striking as it was gained the same month that Brazil and the rest of the Mercosur South American trade bloc finalized a free trade agreement with the European Union. **[1]**

Although in recent years the PRC has emphasized infrastructure-based investment, and while it has deepened its influence in Brazil in the cultural, diasporic, and media spheres, the relationship between the two countries remains skewed toward low value-added commodities exports from Brazil to the PRC. Despite criticisms of the PRC's economic relationship with Brazil made by Brazilian President Jair Bolsonaro during his campaign, hard economic realities ensure that Brazil will not jeopardize its largest commodities export market.

### Criticisms of a Relationship Built on Commodities Exports

Brazil has maintained diplomatic relations with the PRC since 1974. The two countries announced a "strategic partnership" with each other in 1993, and by 2009 China had become Brazil's largest trading partner (China Brief, May 15, 2009; Brazil Ministry of Foreign Affairs, May 2, 2016). The year 2009 also saw the first "BRIC" summit of the leaders of Brazil, Russia, India, and China (later termed BRICS with the addition of South Africa in 2011). The 2014 BRICS summit, hosted in Fortaleza, Brazil, led to the creation of the New Development Bank, a Shanghai-headquartered multilateral development bank within which Brazil controls one-fifth of the voting rights. Brazil will host the five-country BRICS summit in November 2019. In 2020, Brazil is slated to host the fifth annual gathering of the New Development Bank (Brazil Ministry of Economy, April 2, 2019). Without the involvement of Brazil—Latin America's largest economy—the BRICS framework and its attendant New Development Bank would not have a strong anchor in the Americas.

Despite the development cooperation envisioned by BRICS, as well as certain ideological affinities between the PRC and the former governments of Luiz Inacio Lula da Silva and Dilma Rousseff, the frustrations of a Sino-Brazilian relationship predicated on low value-added commodities exports have grown more apparent. Analysts have long noted the negative environmental costs for Brazil from over-reliance on agricultural and mineral exports, as well as limited opportunities to move into higher value-added industries (Stockholm Environment Institute and Global Canopy, December 18, 2018).

Brazilian President Jair Bolsonaro has made statements highly critical of China's economic relationship with Brazil. While still a legislator, Bolsonaro lambasted Brazil's exports of niobium to China for steel alloys (Brazil Chamber of Deputies, September 19, 2016). During Bolsonaro's 2018 presidential campaign (and continuing into office), he frequently repeated the statement that China could "buy in Brazil" but "not buy Brazil" (Valor, April 5, 2019). Bolsonaro has also spoken out against further privatization of Brazil's electricity sector to the PRC's State Grid Corporation of China and State Power Investment Corporation (Valor, October 10, 2018). Bolsonaro was also the first Brazilian president to visit Taiwan, although he did so while still a candidate (Gazeta do Povo, March 9, 2018).

Despite rhetoric critical of the PRC—coupled with overtures to Taiwan—Bolsonaro's economic team promised a pro-business, pro-trade environment unencumbered by the ideological leanings of previous governments. China remains Brazil's largest export market for low value-added commodities such as soybeans, meat, and iron ore. Furthermore, agribusiness has been one of Bolsonaro's core constituencies, and one that has particularly benefited from the export of soybeans to the PRC.

*Image: PRC Ambassador to Brazil, Yang Wanming, meeting with Brazil's Minister of Agriculture, Tereza Cristina, in January 2019. (Source: PRC Consulate in Rio de Janeiro, January 31)*

**China Shifts Its Discourse in Brazil to Infrastructure Investments**

However, while geographically distant from Brazil, the relationship between the PRC and Brazil has never been focused solely on trade. Although the two countries are geographically distant, China's geostrategic concerns remain close to the surface; and even as the existing China-Brazil economic relationship has generated criticism, China has shifted its discourse with respect to Brazil. Discussion of the commodities export relationship has not disappeared, but it has been subsumed into China's public discourse regarding infrastructure development in Brazil. This has also been accompanied by more active PRC outreach in the cultural, diasporic, and media spheres.

In 2017, with the launch of a $20 billion China-Brazil Fund, former PRC Vice Premier Wang Yang stated that investment in Brazil would focus on infrastructure development (PRC Embassy in Brasília, September 3, 2017). The same year Xi Jinping stated to former Brazilian president Michel Temer that the PRC "appreciates" Brazil's long-time adhesion to a "One China" policy, and aims to "synergize" the Belt and Road Initiative (BRI) with Brazil's own development strategies (PRC Embassy in Brasília, September 2, 2017). In 2019, PRC Vice President Wang Qishan also stressed the importance of coupling the BRI to Brazil's development (PRC Embassy in Brasília, May 25, 2019).


*Image: The March 2018 ground-breaking ceremony for the new port facility in São Luís, in northern Brazil. The port construction project is led by the PRC state-owned firm China Communications Construction Company. (Source: PRC State Council Information Office)*

While Chinese public discourse stresses large-scale infrastructure investment, the reality is that much of this investment reinforces the commodities export relationship. PRC companies have shown particular interest in projects that enhance Brazil's infrastructure for the purpose of agricultural and mineral exports. State-owned firms such as China Communications Construction Company have taken particular interest in railroad

concessions for grain transport, and the same company is currently building a port in the northern coastal city of São Luís to expand export cargoes (Xinhua, March 16, 2018; Folha de São Paulo, March 19, 2018).

**Cultural Engagement by Chinese Communist Party Front Organizations**

Less than a quarter of one percent of Brazil's total population is of Chinese descent, most of whom reside in Brazil's largest city of São Paulo. Even with the small size of the Chinese diaspora in Brazil, Chinese Communist Party (CCP) front organizations are present and have a reach that extends beyond Chinese immigrant communities. A notable front group of the CCP, the Council for the Promotion of the Peaceful Reunification of China, is active in São Paulo and Rio de Janeiro (China Brief, May 9, 2019; PRC Ministry of Foreign Affairs, July 4, 2017). The Overseas Chinese Affairs Office, absorbed into the CCP's United Front Work Department (UFWD) in 2018 (China Brief, May 9, 2019), designates the Chinese Association of Brazil (*Associação Chinesa do Brasil*) in São Paulo as its main service organization for overseas Chinese in the country (Overseas Chinese Affairs Office, April 6, 2016).

There are presently 10 Confucius Institutes in Brazil (Confucius Institute Headquarters, July 2, 2019). In contrast to controversies recently seen in North America, Europe, Australia, and elsewhere, critical appraisals of Confucius Institutes are so far virtually non-existent in the Brazilian media. Furthermore, Confucius Institutes have doubled as job fairs for PRC businesses investing in Brazil: this includes surveillance companies like Hikvision and Dahua Technology, and state-run heavy machinery companies, such as XCMG, that benefit directly from BRI projects (Estadão, November 7, 2018).

**The PRC's Growing Engagement with Brazilian Media**

The PRC's state television network China Central Television (CCTV) has had a presence in Brazil since 2010, and Beijing's engagement with Brazilian media has further ramped up in recent years. In 2017, CCTV inked a strategic partnership agreement with one of Brazil's largest private broadcast networks, Rede Bandeirantes (PRC Consulate in São Paulo, December 6, 2017). The following year, the PRC Consulate in São Paulo held its first "Friends of the Press" reception with attendance from two of Brazil's principal newspapers, *Folha de São Paulo* and *Estadão*, alongside Rede Bandeirantes and other media outlets (PRC Consulate in São Paulo, November 10, 2018). The same year *Folha de São Paulo* published a piece by the PRC Consul-General of São Paulo, Chen Peijie, that celebrated the anniversary of the countries' diplomatic relations and characterized the relationship between the two countries as a "friendship that overcomes geographic distance" (PRC Consulate in São Paulo, August 15, 2018).

In 2019, a major Brazilian newspaper based in the country's capital, *Correio Braziliense*, published an article by the Chinese Ambassador to Brazil, Yang Wanming, which stressed the PRC's desire to "create synergy" between the BRI and Brazil's own development, while omitting any mention of commodities in the countries' bilateral relationship (PRC Embassy in Brasília, March 26, 2019). In 2019, Brazil's largest private media

outlet, *O Globo*, pubished an article by the PRC Consul-General of Rio de Janeiro, Li Yang, which also emphasized the importance of the BRI in Sino-Brazilian relations and pointed out Chinese construction of high-voltage power transmission lines for Brazil's Belo Monte Dam (PRC Consulate in Rio de Janeiro, June 4, 2019). Similarly, no mention was made of commodities.

**Conclusion**

Despite China's efforts to diversify its economic relationship with Brazil and to engage in different spheres, Brazilian agricultural exports play a growing role in the PRC's food security. The Bolsonaro government was not about to snub the director-general of FAO, the person who would become the world's foremost advocate of food security. This is all the more apparent as the PRC is the principal buyer of Brazilian meat products, absorbing almost 18 percent of Brazil's total meat exports in 2018 (Brazilian Ministry of Agriculture, March 1, 2019).

The Bolsonaro government has recognized the need to diversify its commercial relationship with China into higher value-added activities such as services and renewable energy (Brazil Ministry of Economy, May 28, 2019; Brazil Ministry of Economy, June 22, 2019). Despite this, commodities exports are expected to grow. As such, criticism of the relationship will continue to surface. Observers of Brazil-China relations should watch for increased PRC presence in the Brazilian media, targeted infrastructure investments in the country, and further cultural engagement by UFWD-affiliated organizations. Such engagements, and investments under the rubric of the BRI, are gradually expanding a relationship that continues to be skewed toward low value-added commodities exports.

*Shanti Salas is a private sector risk consultant who has advised companies on compliance matters for over 15 years. His area of focus is Brazil and he holds an M.A. in Latin American and Caribbean Studies from Florida International University. The views expressed in this piece are the author's own and are not intended to reflect the positions of any organization.*

**Notes**

**[1]** The 2019 EU-Brazil trade agreement, which was finalized after 20 years of negotiations, will reduce tariffs on Brazil's agricultural exports to the European Union (Brazil Ministry of Agriculture, June 28, 2019).

***

ChinaBrief • Volume 19 • Issue 16 • September 6, 2019

# Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations

*By Nathan Beauchamp-Mustafaga*

## Introduction

As information becomes ever more central for Chinese warfighting, the People's Liberation Army (PLA) is developing a new concept for psychological warfare in the information era called "cognitive domain operations" (认知域作战, *renzhiyuzuozhan*). **[1]** This next-generation evolution of psychological warfare seeks to use information to influence an adversary's cognitive functions, spanning from peacetime public opinion to wartime decision-making. The concept is largely inspired by the U.S. military's emphasis on the cognitive domain's decisive role in modern warfare, and the belief among the leaders of the Chinese Communist Party (CCP) that the U.S. government has already used social media to foment political revolutions against authoritarian governments during events such as the Arab Spring. After several years of concerns over China's vulnerabilities in the cognitive domain, the PLA is now developing offensive strategies and capabilities to influence adversary public opinion—as recently evidenced in its political interference in Taiwan's November 2018 elections, and its summer 2019 disinformation campaign against Hong Kong protesters (China Brief, September 6).


*Image: An image published in December 2016 on the official Weibo account of the PLA Air Force. In an apparent effort to shape public perceptions in Taiwan, PRC media sources speculated that the peaks in the background belonged to mountains in Taiwan. (Source: Taiwan News)*

## Overview of Cognitive Domain Operations

Broadly speaking, cognitive domain operations fall under the rubric of psychological warfare, which is itself a part of the PLA's concept of information operations. China already has a wide range of concepts that relate to Western definitions of influence operations, to include: the "three warfares" (三战, *sanzhan*), consisting of

psychological warfare (心理战, *xinlizhan*], public opinion warfare (舆论战, *yulunzhan*], and legal warfare (法律战, *faluzhan*); political warfare (政治战, *zhengzhizhan*); and external propaganda (对外宣传, *duiwai xuanchuan*). **[2]** The PLA is very likely in the early stages of its development of this new capability, based on relatively inconsistent terminology and the PLA's writings on its own perceived shortcomings. What began as fundamentally a wartime concept focused on impacting the adversary's military decision-making process now extends to peacetime operations against entire societies—enabled by the wide reach of modern information technology, and especially social media.

Cognitive domain operations are framed as the next evolution in warfare, moving from the natural and material domains—land, maritime, air, and electromagnetic—into the realm of the human mind. The goal of cognitive domain operations is "mind superiority" (制脑权, *zhinaoquan*), using psychological warfare to shape or even control the enemy's cognitive thinking and decision-making. **[3]** As cognitive domain operations represent the next frontier of warfare domains, mind superiority is the next phase in the evolution of the traditional PLA concept of the three superiorities—sea superiority, air superiority, and information superiority—all of which are necessary for victory. **[4]**

According to a 2017 *PLA Daily* article by the leading PLA theorist Zeng Huafeng of the National University of Defense Technology (NUDT), "cognitive space" is defined as "the area in which feelings, perception, understanding, beliefs, and values exist, and is the field of decision-making through reasoning." It includes many "intangible factors" such as "leadership, morale, cohesion; training level and experience; situational awareness and public opinion." **[5]** Drawing from U.S. subversive psychological operations targeted against the Soviet Union during the Cold War, the article envisions using "information and popular spiritual and cultural products as weapons to influence people's psychology, will, attitude, behavior and even change the ideology, values, cultural traditions and social systems," and " target[ing] individuals, groups, countries, and even people around the world." Zeng identified four tactics to win "mind superiority" in the cognitive space: 1) "perception manipulation" through propaganda narratives; 2) "cutting off historical memory" so that targets will be open to new values; 3) "changing the paradigm of thinking" by targeting elites to change their ideology; and 4) "deconstructing symbols" to challenge national identity. **[6]** For Zeng, cognitive warfare is the ultimate form of winning without fighting.

**Three Phases of PLA Research on Cognitive Domain Operations**

Like many developments in the PLA, cognitive domain operations find their roots in U.S. military operations and doctrine. **[7]** The 2001 Department of Defense report to Congress on "network centric warfare" first introduced the concept of the cognitive domain to go along with the physical and information domains. **[8]** *Information Warfare* (Joint Publication 13-3, released in 2006) further explained that the United States would seek to target the cognitive domain through psychological operations to "influence" adversaries, and further employ military deception to "mislead" them. **[9]** More recently, the U.S. military's "multi-domain operations" explicitly seek to gain the advantage in the cognitive domain. **[10]** In 2005, early PLA writings

conceptualizing the first phase of "operations in the cognitive domain" largely focused on decision-makers' cognitive process and ability in wartime, and did not consider the internet the most significant vector. **[11]**

The second phase (2013-2016) was characterized by PLA concern over the United States using information—especially the internet, and later, social media—to undermine CCP rule in China. Although the PLA first recognized the dangers of social media with the 2009 Iranian protests, concerns were really solidified several years later. This was demonstrated by the research of Zeng Huafeng and Shi Haiming, who coined the idea of "national cognitive security" (国家认知空间安全, *guojia renzhikongjian anquan*) in a 2013 article and a 2014 book on "mind superiority" published by the Academy of Military Science (AMS). **[12]**

In 2015, the National Defense University's (NDU) Science of Military Strategy said, "Since the beginning of the 21st century, cyberspace has been used by some countries to launch 'color revolutions' against other countries… [through] behind-the-scenes operations using social networking sites such as Twitter and Facebook as the engine, from manufacturing network public opinion to inciting social unrest." **[13]** Zeng and Shi were the first in the PLA to identify, at least to a wide audience, the broader potential of the internet for influencing a nation's public opinion at a mass scale. **[14]** It did not take long for the PLA to realize the offensive potential of cognitive domain operations and broaden its theoretical scope to include enemy populations in peacetime—as mentioned in the journals *China Military Science* (in 2016), and *National Defense* (in 2019). It has been cited by researchers from a wide variety of PLA institutions, including SSF Base 311, NUDT, PLARF Engineering University, Army Command College, and the Luoyang Electronic Equipment Test Center. **[15]**

**A Framework for Cognitive Domain Operations**

An August 2018 article by NUDT researchers provides an expansive conceptual framework for cognitive domain operations. It explains that "cognitive domain operations have already become the main battlefield for other countries conducting ideological penetration, and is an important domain for both sides in a war to fight for or destroy troop morale and cohesion, as well as forming or deconstructing operational capabilities." **[16]** The researchers highlight six technologies, divided across two categories, that will be key in leveraging the cognitive domain for political and economic gains. The first category, cognition (阈上认知, *yushangrenzhi*), includes technologies that affect someone's ability to think and function. The second category, subliminal cognition (阈下认知, *yuxiarenzhi*), covers technologies that target a person's underlying emotions, knowledge, willpower and beliefs.

*Cognitive influence technologies*:

1. "Cognitive survey technology" (认知测量技术, *renzhi celiang jishu*) translates psychological indicators into quantifiable signals to assess the adversary's psychological disposition—not only their perceptions, memories, and speech, but also their motivations, emotions, and needs. **[17]**
2. "Cognitive interference technology" (认知干扰技术, *renzhi ganrao jishu*) is used to conduct attacks against the adversary's psychological well-being through lethal and non-lethal means. Light waves, electromagnetic waves, and microwaves, can "cause psychological damage, confusion, and even hallucinations, changing the other's cognition, and ultimately causing the enemy to act in violation of their own interests." **[18]**
3. "Cognitive strengthening technology" (认知强化技术, *renzhi qianghua jishu*) is used to improve one's own cognitive abilities.

*Subliminal cognitive influence technologies:*

1. "Subliminal information processing technology" (阈下认知信息加工技术, *yuxia renzhi xinxi jiagong jishu*) to "collect and pre-treat" content.
2. "Subliminal information implantation technology" (阈下认知信息植入技术, *yuxia renzhi xinxi zhiru jishu*) is used to implant subliminal messages into content, and to create "synthetic information" (合成信息, *hecheng xinxi*).
3. "Subliminal information detection technology" (阈下认知信息检测技术, *yuxia renzhi xinxi jiance jishu*) is presumably to be used for defensive purposes against adversary use of subliminal messaging.

There are indications that China is already deploying at least some of these weapons. The U.S. military has directly accused China of using lasers to blind pilots flying near the PLA base in Djibouti, and has also hinted at their further use by PRC actors in the East China Sea. **[19]** U.S. foreign service officers at the Guangzhou consulate were evacuated in June 2018 with unexplained illnesses that resembled brain injuries following reports of similar attacks in Cuba. **[20]** While no specific country has been blamed, the cause was reportedly attributed to microwave weapons. **[21]** If nothing else, it is clear that the PLA is watching and learning from other militaries deploying these "cognitive interference" technologies in real time.

**Graphic Depictions of U.S. and Chinese Concepts of Cognitive Domain Operations**

The series of graphics presented below depict the evolution of U.S. and Chinese thinking on cognitive domain operations. As may be seen from the graphics, U.S. military and PLA thinking share similar baseline concepts, but the evolving PLA theories move in a far more expansive direction.

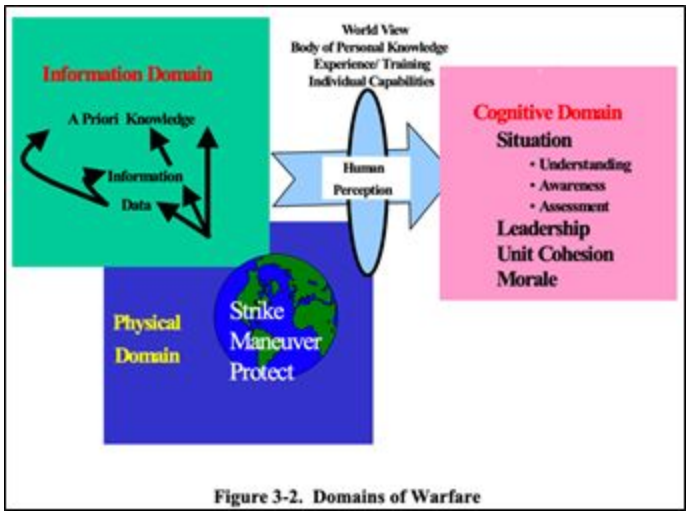



*Image: Initial U.S. Conception of the Cognitive Domain in Warfare.*
(Source: Department of Defense Report to Congress, July 27, 2001.)

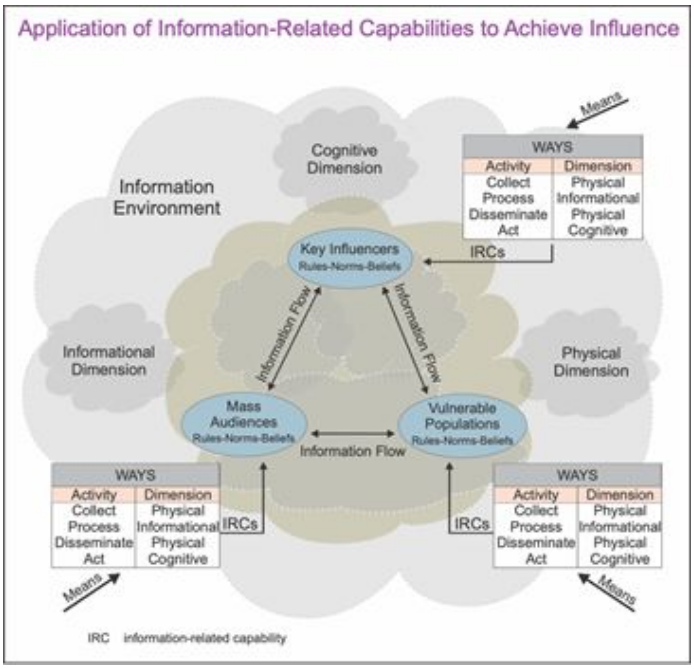



*Image: Recent U.S. Conception of the Role of the Cognitive Domain in Influence Operations.*
*(Source: Joint Chiefs of Staff, November 2012.)*

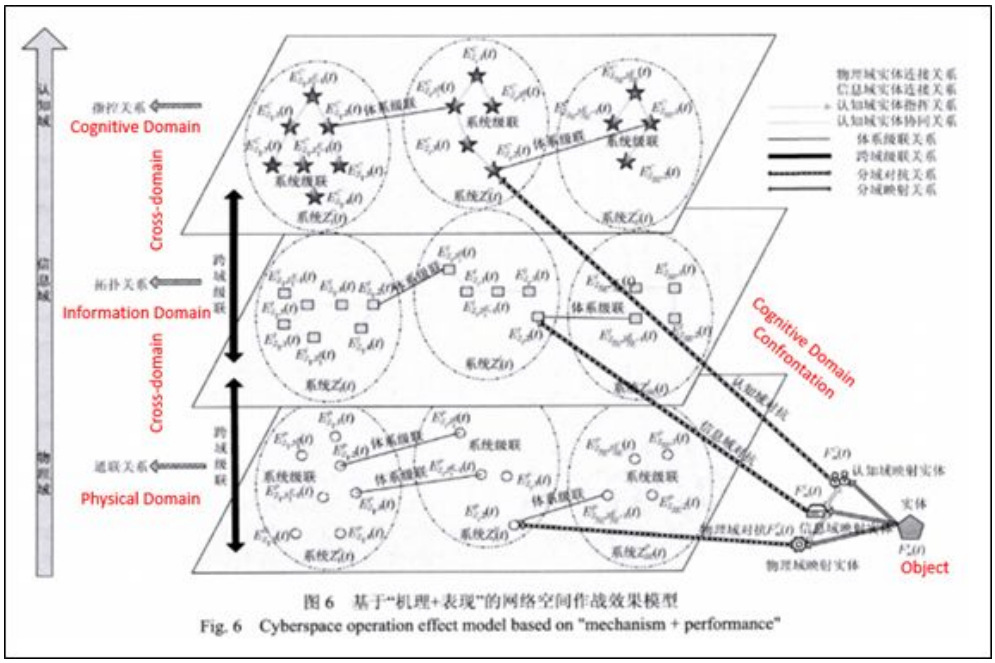



*Image: Chinese Conception of the Role of the Cognitive Domain in Cyber Operations.*
*(Source: Journal of System Simulation, [系统仿真学报] September 2017.)*

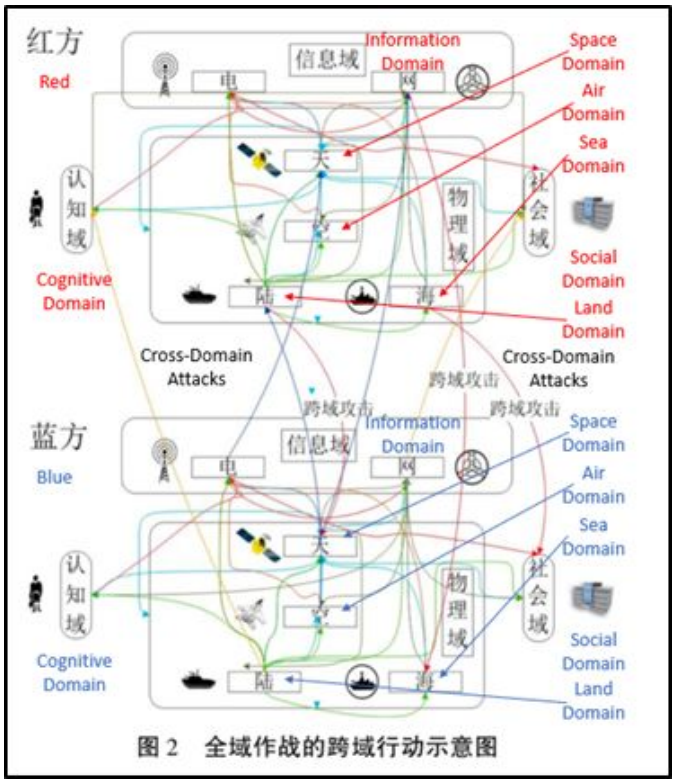



*Image: Chinese Conception of Cognitive Domain Links to Other Domains.*
*(Source: Military Operations Research and Systems Engineering, [军事运筹与系统工程], January 2018.)*

**Offensive Applications of Cognitive Domain Operations**

Solid evidence exists that the PLA is seeking to move into real-world application of cognitive domain operations. One such example is a 2018 article about the hardware requirements for cognitive domain operations. **[22]** The article was written by computer engineers in Base 311 (Unit 61716), the PLA's leading psychological warfare unit under the Strategic Support Force (SSF), which was likely responsible for disinformation during the Taiwan election. Notably, the article was drafted in May and published in October, just as China was ramping up its interference. The article explicitly referenced Facebook, Twitter and LINE—all platforms China reportedly exploited against Taiwan and (except LINE) Hong Kong—and described social media as "a constantly open system that is highly inclusive and transcends the boundaries of national borders, cultural barriers and media." **[23]**

The authors point out several shortcomings that the PLA is facing, and note that the PLA has "little research on the technology and equipment for cognitive domain operations on mainstream social networking platforms." **[24]** They write that China needs to improve its big data, natural language processing, and deep learning capabilities, with multiple goals in mind: conducting subliminal messaging (阈下信息植入, *yuxia xinxi zhiru*), employing "voice information synthesis technology" (语音信息合成, *yuyin xinxi hecheng*), disseminating "network propaganda" (网络宣传, *wangluo xuanchuan*), and analyzing internet users' sentiments.**[ 25]** The article also raises the prospects of buying or renting equipment through military-civil fusion to reduce costs while "ensuring secrecy," and highlights the importance of "improving the overall operational capabilities of professional cognitive domain combat forces." **[26]**

The PLA has also begun patenting technologies dealing with the cognitive domain since at least 2018, again reinforcing the real-world application of this concept. **[27]** These examples clearly indicate the PLA is developing specialized technologies and training personnel to manipulate foreign social media platforms under the rubric of cognitive domain operations.

**A New Holistic Concept Subsuming Previous Research**

Cognitive domain operations now appear to be subsuming many previously distinct lines of effort under the PLA's psychological warfare program. For example, subliminal messaging is specifically referenced as a key technology for cognitive domain operations by the aforementioned 2014 AMS book, 2018 NUDT and 2018 SSF Base 311 articles. There has been a clear line of effort by NUDT over the last 10 years, following the broader PLA shift from a defensive to an offensive mindset, that included research on how to use subliminal messaging to reduce PLA soldiers' resistance to indoctrination. Some of these tactics were recently tested on NUDT students in a class on the "three warfares." **[28]** NDUT researched video manipulation during 2010-2011, and a December 2011 article proposed using " audio-visual technology to imitate the voice of the national leadership and battlefield commanders to mislead the adversary's decision-makers into wrong decisions." **[29]** This video editing required "sound-image synthesis technology" (声像合成技术,

*shengxiang hecheng jishu*)—a term that resembles other PLA references to "voice information synthesis technology," and seems to indicate the development of building blocks for deep fakes. **[30]**

**Disinformation is a Key Feature**

Disinformation (虚假信息, *xujia xinxi*) has always been a component of the PLA's information warfare strategy and appears to be a key, though implicit, feature of cognitive domain operations. **[31]** A 2013 AMS teaching guide for information operations and psychological warfare identifies methods such as "creating information chaos… implanting disinformation and erroneous information into the enemy's information system, and causing the enemy's command to make the wrong decisions and commands" in peacetime and wartime. **[32]** The December 2011 article on video manipulation discusses creating "distorted videos" (篡改视频, *cuangai shipin*), fake videos (虚拟视频, *xuni shipin*) and "videos for deterrence" (视频威慑, *shipin weishe*), even identifying situations and targets for disinformation, including peacetime operations, as shown in the table below. **[33]** This theoretical framework correlates with the PLA Air Force's use of reportedly fake images of H-6K bombers flying close to Taiwanese mountains as propaganda material to threaten Taiwan. **[34]**

***Specific Recommendations for Targeting of Disinformation by PLA Researchers:***

| Operational Phase | Operational Target | Tactics | Information Type | Vector | Operational Goal |
|---|---|---|---|---|---|
| Peacetime | Domestic Masses | National Programming Plan | Truthful | | • Strengthening domestic confidence<br>• International public opinion support |
| | International Society | | | | |
| Wartime | Adversary Elites | Edit video content | Truthful + disinformation | EW interference | •Oppose War<br>•Pressure wartime psychology<br>•[Induce] commanders' incorrect decisions |
| | Battlefield Troops | Selectively broadcast true information | Truthful | Internet penetration | |
| | Masses | Pure disinformation | Disinformation | | |

*Image: Specific Recommendations for Targeting of Disinformation by PLA Researchers.*
(Source: Fire Control and Command Control [火力与指挥控制], December 2011.)

**Real World Evidence**

Taiwan is the best case study of the real-world applications of the PLA's cognitive domain operations, and highlights one clear vector: social media disinformation. The Taiwan government has claimed that China

interfered with the island's November 2018 election through a variety of means, employing both traditional and social media. **[35]** Anonymous Taiwanese national security officials have claimed the SSF was the driving force behind the election interference campaign, and reports have identified Beijing artificially generating support for its preferred candidates on social media. **[36]** Researchers have suggested the CCP Propaganda Department, CCP United Front Work Department, and perhaps private contractors could have played a role as well. **[37]**

One PLA article provides insight into how the Chinese military may have prepared for cognitive domain operations against Taiwan. A 2017 article by a graduate student at the Nanjing Political Institute (now under NDU as the military institution's Political Academy) created a playbook for how the Chinese military could "localize" "targeted communications" towards Taiwan on social media. **[38]** The author specifically focuses the article on PTT, a popular Reddit-like Taiwanese bulletin board service, and explains how to alter typical mainland Mandarin sentence structure and vocabulary to sound more like that of Southern Min, the dialect used in Taiwan. The author adds that sounding local will reduce the emotional distance between the two sides, otherwise it is "very easy to spot and will attract the attention of other Internet users." **[39]**

**Conclusion**

Cognitive domain operations appear to be the key operational concept behind China's embrace of social media disinformation. Chinese information operations and psychological warfare—what the West would call influence operations—have a long history, and it should come as no surprise that the CCP is embracing the newest and most effective tools for mass communications. Social media could greatly increase the ability of the PLA to target tailored messaging to specific audiences based on artificial intelligence (AI) and big data analytics. For example, a June 2019 article co-authored by SSF Base 311 personnel called for the PLA to abandon the use of "sockpuppets" (马甲, *majia*), or false online identities used for deception, in favor of AI-enabled "intelligent public opinion guidance" (网络舆情智能引导, *wangluoyuqing zhinengyindao*) software that has the ability to automatically and adaptively generate content and select the optimal time and method for coordinated posts. **[40]** It remains to be seen how effective China will be in capitalizing on these capabilities. The experience of Taiwan, combined with recent reports of Chinese state-backed disinformation campaigns against Hong Kong, suggests that CCP efforts in this realm are just getting started. It is worth wondering where the PLA will employ its cognitive domain operations toolkit next.

*Nathan Beauchamp-Mustafaga is a Policy Analyst at the nonprofit, nonpartisan RAND Corporation. He is currently working on a larger report with Michael Chase for the Foreign Policy Institute at Johns Hopkins SAIS on how the Chinese military uses social media for influence operations.*

**Notes**

**[1]** Other permutations include 认知领域作战 (*renzhilingyuzuozhan*) and 认知空间作战 (*renzhikongjianzuozhan*). For related research, see: Rachael Burton, "Disinformation in Taiwan and Cognitive Warfare," *Global Taiwan Brief*, November 14, 2018, http://globaltaiwan.org/2018/11/vol-3-issue-22/.

**[2]** For more on PLA influence operations via propaganda and political warfare, see: David Shambaugh, "China's Propaganda System: Institutions, Processes and Efficacy," *The China Journal* 57, 2007, pp. 25–58; Wang Juntao and Anne-Marie Brady, "Sword and Pen: The Propaganda System of the People's Liberation Army" in Anne-Marie Brady, ed, *China's Thought Management* (London, UK: Routledge, 2011); Mark Stokes and Russell Hsiao, "The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics," Project 2049 Institute, October 14, 2013, https://www.project2049.net/documents/PLA_General_Political_Department_Liaison_Stokes_Hsiao.pdf; Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief*, August 22, 2016, https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/; Elsa Kania, "China's War for Narrative Dominance," *National Interest*, May 28, 2017, https://nationalinterest.org/blog/the-buzz/why-chinas-three-warfares-could-provide-beijing-big-gains-20878; Peter Mattis, "China's 'Three Warfares' In Perspective," *War on the Rocks*, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

**[3]** 制脑权 can also be translated as "brain control," which is a term used by the PLA to mean achieving human-machine integration, such as controlling machines with human brains and improving artificial intelligence (AI) by modeling the brain. See: Song Wen [宋文], Liang Ningning [梁宁宁], and Yang Kegong [杨克功], "Brain Project: A New Height in World Technology Competition" ["脑计划：世界科技竞争新高地"], *PLA Daily*, October 20, 2016, http://www.81.cn/jfjbmap/content/2016-10/20/content_159464.htm; Elsa Kania, "PLA Human-Machine Integration (人机融合)," CNAS, undated. This has also been referred to as "intelligence control" (制智权). See: Shen Shoulin [沈寿林] and Zhang Guoning [张国宁], "Intelligent Knowledge Operations" ["认识智能化作战"], PLA Daily, March 1, 2018, http://www.81.cn/jfjbmap/content/2018-03/01/content_200671.htm.

**[4]** For background on the three superiorities, see: Zhang Yuliang [张玉良], ed., *The Science of Campaigns* [战役学] (Beijing, China: National Defense University Press [国防大学出版社], 2006), pp. 80.

**[5]** Zhu Xueling [朱雪玲] and Zeng Huafeng [曾华锋], "Mind Control Operations: New Model of Future Wars" ["制脑作战：未来战争竞争新模式"], *PLA Daily*, October 17, 2017, http://www.81.cn/jfjbmap/content/2017-10/17/content_189879.htm.

**[6]** Zeng Huafeng [曾华锋] interviewed by Huang Kunlun [黄昆仑], "Seizing Mind Superiority in Future Wars" ["夺取未来战争 制脑权"], *PLA Daily*, June 16, 2014, http://www.81.cn/jwgd/2014-06/16/content_5961384.htm.

**[7]** Many of these early writings appear to draw from one book: Che Xianming [车先明] and Chen Xuehui [陈学惠], *U.S. Operations Theory* [美军作战理论] (Beijing, China: Academy of Military Science Press [军事科学出版社], 2005).

**[8]** *Network Centric Warfare* (Arlington, VA: Department of Defense, report to Congress, July 27, 2001), http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf.

**[9]** Joint Chiefs of Staff, *Information Operations* (Arlington, VA: Department of Defense, February 2006), https://www.hsdl.org/?abstract&did=461648.

**[10]** The article cites the November 2016 *U.S. Army Doctrine Reference Publication 3-0* as unveiling the multi-domain battle concept, which is true, but then wrongly states that it focuses on seizing the advantage in the cognitive domain. It appears the authors were relying on other PLA sources. See: *Operations: Army Doctrine Reference Publication 3-0* (Headquarters, Department of the Army, November 2016), https://usacac.army.mil/sites/default/files/publications/ADRP%203-0%20OPERATIONS%2011NOV16.pdf. For the latest strategy, see: *TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028* (U.S. Army Training and Doctrine Command, December 2018), https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

**[11]** See: Zhao Liang [赵亮] and Luo Xueshan [罗雪山], "Research on Collaboration and Its Quantifiable Model in the Network Centric Warfare" ["网络中心战中的协作及其量化模型研究"], *Intelligence Command Control and Simulation Techniques* [情报指挥控制系统与仿真技术], December 2005.

**[12]** For an article on the 2009 Iranian protests, see: Chi Yannian [迟延年], "Cyber Subversion: Security Threats That Must Not Be Taken Lightly" ["网络颠覆: 不容小觑的安全威胁"], *China Defense News*, August 6, 2009, pp. 3. Zeng and Shi first used the term in 2011 but presented the comprehensive concept in 2013. Shi Haiming [石海明] and Zeng Huafeng [曾华锋], "The Communication of Military Technology: Visual Image, Cognition and War" [军事科技传播: 视像、认知与战争], Jour*nal of Changsha University of Science and Technology (Social Science)* [长沙理工大学学报 (社会科学版)], July 2011; Zeng Huafeng [曾华锋] and Shi Haiming [石海明], "On National Cognitive Space Security Strategy" [论国家认知空间安全战略], *Theoretical Studies on PLA Political Work* [军队政工理论研究], May 2013. For the 2014 book, see: Zeng Huafeng [曾华锋] and Shi Haiming [石海明], *Mind Superiority: The Rules of War and National Security Strategy in the Global Media Age* [制脑权: 全球媒体时代的战争法则与国家安全战略] (Beijing, China: Academy of Military Science Press, 2014).

**[13]** Xiao Tianliang, ed. [肖天亮], *Science of Military Strategy* [战略学] (Beijing: National Defense University Publishing House [北京国防大学出版社], 2015). Translation via Nathan Beauchamp-Mustafaga and Michael Chase, Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations (Washington, DC: John Hopkins SAIS, forthcoming). Others have said China is already at war in the cognitive domain: Li Donghang [李东航], "We're Already in a War for Mind Superiority" ["我们已然身处一场制脑权战争中"], *PLA Daily*, May 22, 2015, http://www.81.cn/2015hwyx/2015-05/22/content_6503212.htm. For more concerns about political revolutions, see: Lan Zhouda [兰舟达] and Ma Jianguang [马建光], "New Cyber Warfare From The Perspective Of Mind Superiority: Taking The Color Revolutions As An Example" ["制脑权视野下的新型网络战: 以颜色革命为例"], *Defense Technology Review* [国防科技], April 2015, pp. 57-62.

**[14]** An earlier PLA book I did not have access to is: Lu Jixuan [逯记选], *The Radiating Summit of Psychological Warfare: Research on Cognitive Domain Operations in Modern Warfare* [心战之巅的光芒: 现代战争中的认知域作战研究] (Shenyang: Baishan Press [白山出版社], 2012). This is cited less frequently in PLA articles than Zeng and Shi's book.

**[15]** See: Shi Zhongwu [石忠武], "Considerations on Promoting the Transformation of the PLA Army" ["推进陆军转型建设的几点思考"], *China Military Science* [中国军事科学], December 2016; Zhang Fang [张芳] and Wei Jiying [魏际英], "Enhancing the aggressiveness and initiative of military strategy communication under the media fusion communication environment" ["媒体融合传播环境下增强军事战略传播进取性和主动性问题"], *Course Education Research* [课程教育研究], March 2019; Lu Hongwei [路红卫], "Revisiting the Essential Feature of Modern War" ["再谈现代战争的本质特征"], *National Defense* [国防], May 2019.

**[16]** Luo Yuzhen [罗语嫣], Li Wei [李璜], Wang Ruifa [王瑞发], Lei Wei [雷潇], Liao Dongsheng [廖东升], and Zhu Yingying [朱莹莹], "Characteristics and Key Technologies of the Common Domain for the Cognitive Domain" ["认知域的公域特性及其关键技术"], *Defense Technology Review* [国防科技], April 2018.

**[17]** For one likely example of this effort, see: Wang Ruifa [王瑞发], Luo Yuyan [罗语嫣], and Liao Dongsheng [廖东升], "Cognitive modeling and its implication for psychological warfare" ["认知建模及其心理战"], *Defense Technology Review* [国防科技 ], March 2018.

**[18]** Specific "psychological warfare weapons" (心理战武器) include, "electromagnetic wave weapons" (电磁波武器), "infrasound weapons" (次声武器), "neuro-infrasound weapons" (神经型次声波武器) because they can cause "confusion and madness," and "can influence and control the human hearing, and finally achieve the purpose of disturbing the human mind"; and "laser blinding weapons" (激光致盲武器).

**[19]** Gordon Lubold and Jeremy Page, "Laser From Chinese Base Aimed at U.S. Military Pilots In Africa's Skies, Pentagon Charges," *Wall Street Journal*, May 3, 2018, https://www.wsj.com/articles/laser-from-chinese-base-aimed-at-u-s-military-pilots-in-africas-skies-pentagon-charges-152535177; Gordon Lubold and Jeremy Page, "American Military Aircraft Targeted By Lasers in Pacific Ocean, U.S. Officials Say," *Wall Street Journal*, June 21, 2018, https://www.wsj.com/articles/american-military-aircraft-targeted-by-lasers-in-pacific-ocean-u-s-officials-say-1529613999. The problem is not only from China, however: Gordon Lubold, "Laser Beam Attacks Bedevil U.S. Military Pilots in Mideast," *Wall Street Journal*, August 17, 2018, https://www.c4isrnet.com/electronic-warfare/2018/04/27/whos-testing-a-laser-in-djibouti/.

**[20]** Steven Lee Myers and Jane Perlez, "U.S. Diplomats Evacuated in China as Medical Mystery Grows," *New York Times*, June 6, 2018, https://www.nytimes.com/2018/06/06/world/asia/china-guangzhou-consulate-sonic-attack.html.

**[21]** William J. Broad, "Microwave Weapons Are Prime Suspect in Ills of U.S. Embassy Workers," *New York Times*, September 1, 2018, https://www.nytimes.com/2018/09/01/science/sonic-attack-cuba-microwave.html.

**[22]** Liu Huiyan [刘惠燕], Xiong Wu [熊武], Wu Xianliang [吴显亮], and Mei Shunliang [ 梅顺量], "Several thoughts on promoting the construction of cognitive domain operations equipment in the whole environment" ["全媒体环境下推进认知域作战装备发展的几点思考"], *Defense Technology Review* [国防科技], October 2018.

**[23]** Ibid.

**[24]** Ibid.

**[25]** For other relevant articles, see: Zhu Xueling [朱雪玲], Lei Xiao [雷潇], and Wen Pei [文旆], "Subliminal Emotional Face and Its brain mechanism" ["阈下情绪面孔及其脑机制"], *Defense Technology Review* [国防科技 ], July 2013; Liao Dongsheng [廖东升] and Liu Jifeng [刘戟锋], "A Review of Subliminal IT Research" ["阈下信息技术研究现状"], *Defense Technology Review* [国防科技 ], July 2013; Liu Fujun [刘付军], "Theoretical analysis of the influence of subliminal information" ["阈下信息影响理论探析"], *Defense Technology Review* [国防科技 ], November 2016; Yang Fei [仰斐] and Liao Dongsheng [廖东升], "Subliminal auditory technology and its application" ["阈下听觉技术研究及其应用"], *Defense Technology Review* [国防科技], January 2017; Lu Hongwei [路红卫, "Revisiting the Essential Feature of Modern War" ["再谈现代战争的本质特征"], *National Defense* [国防], May 2019.

**[26]** Liu, Xiong, et al., "Several thoughts on promoting the construction of cognitive domain operations in the whole environment," *Defense Technology Review* [国防科技], October 2018.

**[27]** For patent from researchers at the SSF's Aeronautical Engineering College and NUDT, see: Hu Min [胡敏] et al, "Method for parallel calculation of safety management in complex space system" ["种复杂空间系统安全管理平行计算方法"], Chinese Patent No. CN107871047A, April 3, 2018; Lei Yonglin [雷永林], "New-type combat effectiveness simulation modeling method" ["种新型作战效能仿真建模方法"], Chinese Patent No. CN107967134A, April 27, 2018; "A kind of equipment cognitive domain understandability appraisal procedure based on maturity" ["一种基于成熟度的装备认知域理解能力评估方法"], Chinese Patent No. CN109615259A, April 12, 2019.

**[28]** Cheng Lingli [陈玲丽], Gong Bo [龚波] and Liu Wen [刘文], "The Cultivation of Core Values of Contemporary Revolutionary Soldiers Based on Subliminal Priming Technology" ["基于阈下启动技术的当代革命军人核心价值观培育"], *Defense Technology Review* [国防科技 ], August 2013.

**[29]** Bu Jiang [卜江], Lao Songyang [老松杨], Bai Liang [白亮], Guo Xiaoyi [郭小一] and Liu Haitao [刘海涛], "The Research on Video Based Psychological Warfare and its Key Technology" ["基于视频的心理战及其关键技术"], *Fire Control and Command Control* [火力与指挥控制], December 2011.

**[30]** For an early reference to synthesis technology and media for psychological warfare, see: Yang Chengping [杨成平] and He Wei [何秧], "The Main Contradictions and Countermeasures in Wartime Political Work" ["战时政治工作面临的主要矛盾及对策"], *Journal of Political Work* [政工学刊], November 2007.

**[31]** For other explicit references to targeting disinformation against adversaries, see: Jia Qingshuai [贾庆帅], Yu Guohe [于国荷], Li Lang [李浪], and Jing Yanhua [井彦华], "Talking about the Application of Psychological Warfare under the Condition of Information Warfare" ["浅谈信息化战争条件下心理战运用手段"], conference paper for the China Medical Education Association's Innovation Research and Chronic Disease Prevention and Control Symposium, August 2012; Gan Yi [甘翼], Nan Jianshe [南建设], Huang Jinyuan [黄金元], Li Gui [李贵], "Research on Information Operation Architecture and Key Technologies" ["信息作战体系架构及关键技术"], *Command Control & Simulation* [指挥控制与仿真], January 2018.

**[32]** Ye Zheng [叶征], *Lectures on the Science of Information Operations* [信息作战学教程] (Beijing, China: Academy of Military Science Press, 2013), p. 105.

**[33]** Bu Jiang [卜江], Lao Songyang [老松杨], Bai Liang [白亮], Guo Xiaoyi [郭小一] and Liu Haitao [刘海涛], "The Research on Video Based Psychological Warfare and its Key Technology" ["基于视频的心理战及其关键技术"], *Fire Control and Command Control* [火力与指挥控制], December 2011.

**[34]** Chien Li-chung, Chung Li-hua and Jonathan Chin, "China using fake news to divide Taiwan," *Taipei Times*, September 16, 2018, http://www.taipeitimes.com/News/front/archives/2018/09/16/2003700513/1; Matthew Strong, "Military denies Yushan in China bomber picture: Peak likely to be Mount Beidawu in Southern Taiwan: experts," *Taiwan News*, December 17, 2016, https://www.taiwannews.com.tw/en/news/3053731.

**[35]** For specific Taiwanese reference to PLA and the cognitive domain, see Chang Ling-ling [張玲玲], "China is at war in the 'cognitive domain,'" *Taipei Times*, May 25, 2019, http://www.taipeitimes.com/News/editorials/archives/2019/05/25/2003715746/1.

**[36]** Chung Li-hua and William Hetherington, "China targets polls with fake accounts," *Taipei Times*, November 5, 2018, http://www.taipeitimes.com/News/front/archives/2018/11/05/2003703618; Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy*, June 26, 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

**[37]** Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy*, June 26, 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.
Perhaps it should not be a surprise that China would contract some of its influence operations to private companies—it has already done so with cyber through the Ministry of State Security (MSS), and even the U.S. Joint Staff's 2006 *Information Operations* says U.S. businesses will assist in psychological operations targeting the cognitive domain.

**[38]** Lai Dongwei [赖东威], "An Analysis of the Minnan Language Sentence Patterns and Vocabulary Used on Taiwanese Social Media" ["台湾社交媒体的闽南语句式和词汇使用现象探析"], *News Research* [新闻研究], November 2017.

**[39]** Ibid.

**[40]** Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Ya [熊尧], "Intelligent agent model for network public opinion guidance" ["网络舆情引导智能代理模型"], *Defense Technology Review* [国防科技], June 2019. Li and Xiong are Huaqiao University's College of Computer Science and Technology, based in Fujian close to Base 311.

***